Project 2

Quantitative Usability Evaluation

Team 15

Ryan Samaroo, Heela Bangash, Frerik Drumm,

Sammy Diamantstein, and Brandon Esford

Submitted to:
Dr. Robert Biddle
COMP3008 Human Computer Interaction
School of Computer Science
Carleton University

April 9th 2018

Contents

1: Sample Data and Descriptive Statistics

- Advantages and Disadvantages of Text21 and Imagept21
  - Text21
  - Imagept21
- Log Data Processing
  - Explanation for your approach
  - PsuedoCode
- Usability and Statistical Analysis
  - Pseudocode
  - Descriptive Statistics
    - Scheme Statistics
    - User Statistics
  - Graphs
    - Total Number of Logins
      - Histograms
    - Login Times Per User
      - Histograms
      - Box plots
  - Interpretation

2: Design, Implementation, Statistical Inference

- Scheme Rationale
- Scheme Implementation
- Quantitative Testing Framework
  - Preface To Quantitative Testing Framework
  - Screenshots of Testing Framework

Questionnaire

Comparison with Text21

3: Appendix

Consent Forms

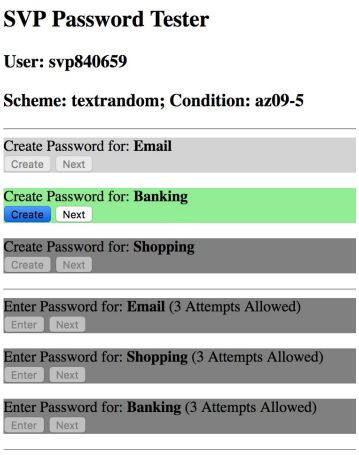
1: Sample Data and Descriptive Statistics

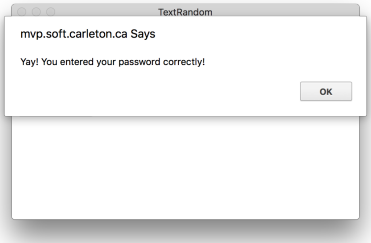
Advantages and Disadvantages of Text21 and Imagept21

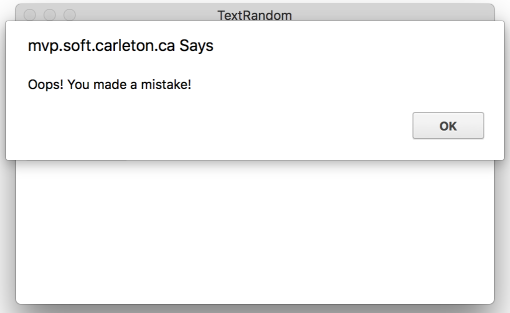
Text21

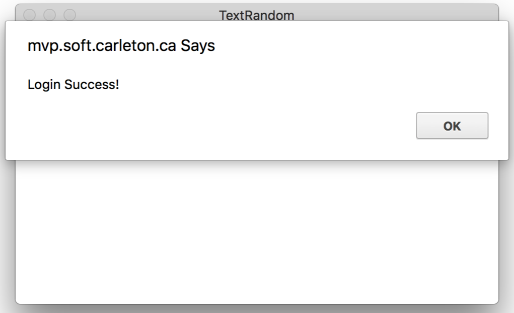
For Text21, it provides a very basic command line or textbox interface which would be familiar to most users in terms of its use. With the generation of new passwords, it limits the length of the password down to 5 characters being a mix of numeric and alphabetic. The length allows the user to ‘chunk’ the alphabetic characters together about the numeric positions to allow for processing into LTS, ie. The password ‘uwmn5’ can be chunked into memory as “You women 5” or ‘i8kw2’ can be “I 8 kiwi 2”.

Although the Text21 password generation is convenient and simple to use, it does have its downfalls. In terms of security, it would be possible to brute-force or determine all (< 36^3 * 10 * 26) possible password combinations since the password follows a certain scheme and it’s just the generation of characters which a computer could go through and create and then input into the password field and run. For some users, it can be harder to remember because they didn’t get to choose their password and there is no feeling of choice / control being given. Many users would resort to writing the passwords down or storing them somewhere on a phone or computer which defeats the purpose of having a short 5 character password. If the password is going to be stored elsewhere, it might as well be a lot longer since ease of memorability is no longer an issue.







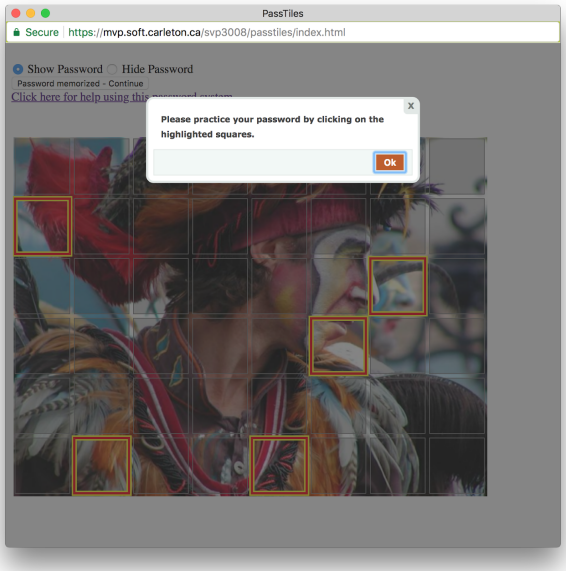


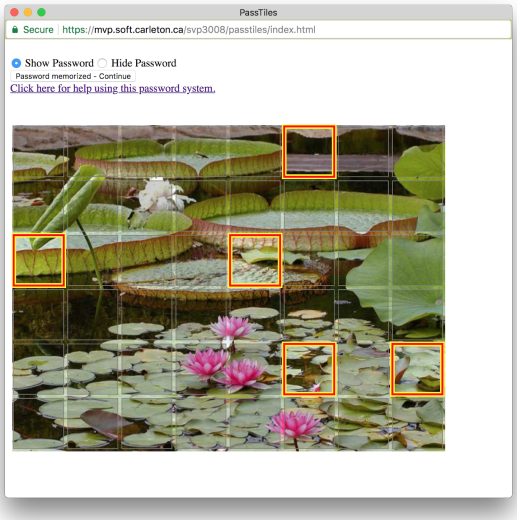
Imagept21

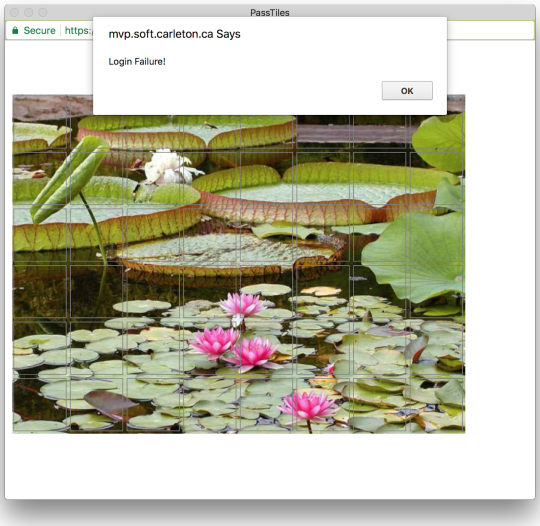
For Imagept21, it provides a graphical interface which would be a bit unfamiliar to most users in terms of its use because most password systems implemented as text-based. The convenience of using this system is the length of the password is 5 image tiles, which translates into a 10 character password, as each tile is made up of an x and y coordinate. The individual tile can be of an object and allows the user to memorize what they clicked on when setting up the password. By recognition, the user can see the image as a whole or by parts and click on tiles that feel familiar to them because of their episodic memory. In general, it is much easier to memorize images than characters and numbers for the majority of people, which could lead to users of this scheme being much more successful in remembering passwords. In terms of security, the images are arbitrary allowing no relation to what the password is meant for, the grid could be

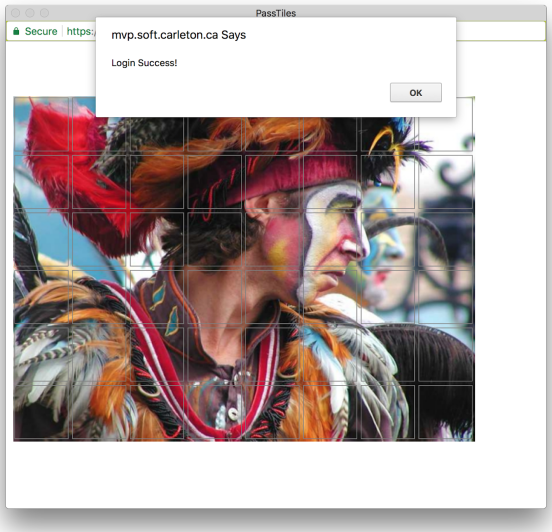
expanded to contain more tiles allowing for more combinations of passwords to be inputted, and the system relies on click events for password input which would be hard to program a computer to enter possible combinations.

In terms of its cons, it could be easily forgotten because of the complexity of the grid or because of what tile was selected in the image, ie. one tile containing snow but all tiles are it are also containing snow. Now this could be resolved with the user memorizing positions of the tiles but these could be forgotten because you're trying to remember 5 coordinates so effectively 10 numbers in a given order. Also, for memorization it would require a series of repetition or password regeneration which would take some time and the user would be upset with having to go through all that work for one password. Although it is a positive but providing arbitrary images to the user with no option of selection doesn't allow them to make connection between the image and the password. Also, there is no visual indicator to show you which tiles you have clicked while entering a password, or indication on how many tiles you have left to click, which can increase the difficulty of entering a password. Even if the password has been remembered correctly, a user may have unintentionally clicked on a tile or a click they thought they made may have not registered. Therefore, highlighting tiles as users click them when entering a password would be a simple improvement to help the user when entering their password.









Log Data Processing

Explanation for your approach

The log processing software we developed generates two CSV files, dataByUser.csv and dataBySite.csv, from the log data files for both schemes provided. The

dataByUser.csv organizes the data obtained by user and contains the information in the following format:

userID, password scheme, total number of logins, number of successful logins, number of failed logins, total number of seconds to enter password during login, total seconds for successful logins, total seconds for failed logins, number of passwords created, number of times the user practiced entering passwords, list of all the login test times, list of successful test times, list of unsuccessful test times

The dataBySite.csv organizes the data obtained by website and contains the information in the following format:

webID, password scheme, total number of logins, number of successful logins, number of failed logins, total number of seconds to enter password during login, total seconds for successful logins, total seconds for failed logins, number of passwords created, number of times the password was practiced during creation, list of all the login test times, list of successful test times, list of unsuccessful test times

The number of times the user practiced the password refers the number of times the user practiced entering the password during the password creation phase. If a user decided to create a new password to replace an existing password the practices were reset so that the number stored only represents the number of times the accepted password that will be used in testing is practiced. The lists of login times were included so they could be used to calculate the mean, median, and standard deviation for the login times for each user as well as for each site/scheme.

The purpose of creating two different csv files was to have the data organised by user as well as organised by site, which simplified the creation of descriptive statistics and graphs when analyzing the csv files using R.

PsuedoCode

The log processing software first generates the dataByUser.csv by analyzing the log data for each scheme line by line as follows:

for each line **in** log data file:

```
get userID;
get password scheme;
while userID remains the same:
    if a new password is created:
        increment # of passwords created for that webID;
        reset # of practices for the password to 0 for that webID;
    if a password is practiced:
        increment the # of practices for that webID;
    if a test is performed:
        record the webID, difference between password start and
        enter timestamps, and if the login was a success or failure in
        a temporary CSV to be used to help create dataByUser.csv as
        well as storing the times in separate hashmaps for success
        and failure to be used in generating dataByUser.csv
if userID changes:
    generate a line in the dataByUser.csv file in the format specified
    previously for the old user using data collected;
```

The log processing software then generates the dataBySite.csv by analyzing the temporary csv with the data for each login test, line by line as follows:

```
for each line in csv file:
    if test successful:
        increment number of successful logins for the webID;
        add the time it took to enter the password to successful login times;
        append the time it took to enter the password to the list of successful
        test times;
    if test failed:
        increment number of failed logins for the webID;
        add the time it took to enter the password to failed login times;
        append the time it took to enter the password to the list of
        unsuccessful test
        times
```

generate dataBySite.csv file by organizing data collected in the format specified previously;

In the creation of both csv files, the total number of logins, total number of seconds to enter password during login, and list of all the login test times were obtained by simply adding (or appending) their respective values for successful and unsuccessful logins.

Usability and Statistical Analysis

Analysis of the usability associated with each password scheme was facilitated through the use of a second software systems called Scheme Comparison. Scheme Comparison is a simple system written in the R programming language that processes the dataByUser.csv and dataByUser.csv files produced by the Log Processor for the purposes of statistical analysis. Specifically, this software reads these files, generates descriptive statistical data for user logins and login times, and then produces histograms and boxplots with respect to this data.

Pseudocode

The logic of the Scheme Comparison may represented language agnostically in the following pseudocode implementation:

```
Algorithm AnalyzeUserdata():
      userData <- Read user data from dataByuser.csv and
      dataBySite.csv.
      scheme1Table <- BuildScheme1Table(userData)
      scheme2Table <- BuildScheme2Table(userData)
      userStats <- BuildUserStatsTable(userData)
      schemeStats <- BuildSchemeStats(userData)

      output userStats to file.
      output schemeStats to file.

      BuildHistogramUserLogins(scheme1Table)
      BuildHistogramUserLogins(scheme2Table)

      BuildHistogramUserLoginTimes(scheme1Table)
      BuildHistogramUserLoginTimes(scheme2Table)
```

```
      BuildBoxPlotUserLoginTimes(userData)
      BuildBoxPlotPerUserLoginTimes(userData)

Subroutine BuildScheme1Table(data):
    return subset of data with only scheme1 entries

Subroutine BuildScheme2Table(data):
    return subset of data with only scheme2 entries

Subroutine BuildUserStatsTable(data):
      stats <- new table with entries computed from data:
            mean, median, mode total login times.
            mean, median, mode successful login times.
            mean, median, mode unsuccessful login times.
            mean, median, mode total logins.
            mean, median, mode successful logins.
            mean, median, mode unsuccessful logins.
      return stats

Subroutine BuildSchemeStats(data):
      stats <- new table with entries compute from data:
            mean, median, mode total login times.
            mean, median, mode successful login times.
            mean, median, mode unsuccessful login times.
            mean, median, mode total logins.
            mean, median, mode successful logins.
            mean, median, mode unsuccessful logins.
            mean, median, mode passwords created
            mean, median, mode number of practice entries.
      return stats

Subroutine BuildHistogramUserLoginTimes(data):
      Construct histogram For total login times and output to
      file.
      Construct histogram For successful login times and output to
      file.
      Construct histogram For unsuccessful login times and output
      to file.

Subroutine BuildHistogramUserLogins(data):
      Construct histogram For total logins and output to file.
      Construct histogram For successful logins and output to
      file.
```

```
        Construct histogram For unsuccessful logins and output to
        file.

    Subroutine BuildBoxPlotUserLoginTimes(data):
        Construct boxplot For total login times and output to file.
        Construct boxplot For successful login times and output to
        file.
        Construct boxplot For unsuccessful login times and output to
        file.
```

Descriptive Statistics

The tables below summarize the descriptive statistics computed from the data contained within the dataByUser.csv and dataBySite.csv files. The contents of this table were obtained from schemeStats.csv and userStats.csv files generated by the Scheme Comparison software. It should be noted that the schemes testpasstiles and testtextrandom extracted from the these csv files refer to Imagept21 and Text21, respectively. Each of the statistics follow the naming convention in which the name of the value is preceded by the statistic it represents. Specifically, mn is used to denote mean, med is used to denote median, and sd is used to denote standard deviation.

Scheme Statistics

Scheme	TotalLogs.mn	TotalLogs.med	TotalLogs.sd	SuccLogs.mn	SuccLogs.med	SuccLogs.sd	FailLogs.mn	FailLogs.med	FailLogs.sd
testpasstiles	15.266667	15	4.463609	11.933333	12	1.334523	3.333333	2	3.677473
testtextrandom	12.277778	12	4.253795	11	12	3.360672	1.277778	0	2.13667

TotalLogTime.mn	TotalLogTime.med	TotalLogTime.sd	SuccLogTime.mn	SuccLogTime.med	SuccLogTime.sd	FailLogTime.mn	FailLogTime.med
17488.93333	298	66599.60963	17424.33333	252	66617.47728	64.6	47
123.55556	95	69.85213	108.05556	95	57.00823	15.5	0

FailLogTime.sd	PasswordsCreat	PasswordsCreat	PasswordsCreat	NumPractices.m	NumPractices.m	NumPractices.sd	TotalTestTimes.	TotalTestTimes.	TotalTestTimes.s

	ed.mn	ed.med	ed.sd	n	ed		mn	med	d
59.92114	5.666667	5	3.457222	5.2666667	4	4.0438077	17.533333	17	7.881866
32.5599	4.166667	4	1.581139	6.1666667	6	0.3834825	16.555556	17.5	11.152537

SuccessfulTestTimes.mn	SuccessfulTestTimes.med	SuccessfulTestTimes.sd	UnsuccessfulTestTimes.mn	UnsuccessfulTestTimes.med	UnsuccessfulTestTimes.sd
17.533333	17	7.881866	9.8	10	6.930265
16.555556	17.5	11.152537	4.222222	1	5.139874

User Statistics

uID	Scheme	TotalTestTime.mn	TotalTestTime.med	TotalTestTime.sd	SuccTestTimes.mn
ast103	testtextrandom	12.5	4.5	14.32990418	12.15384615
ast104	testtextrandom	11.64285714	10.5	3.835204194	11.46153846
ast105	testtextrandom	7.454545455	7	2.769968822	7.222222222
ast107	testtextrandom	5.222222222	4	2.839957654	5.083333333
ast108	testtextrandom	2.933333333	3	1.222799287	2.933333333
ast111	testtextrandom	25.33333333	9	52.02643559	25.33333333
ast112	testtextrandom	8	7	2.256304299	8
ast114	testtextrandom	11.29411765	11	4.05839725	11.5
ast115	testtextrandom	10.66666667	10	3.869069264	10.66666667
ast116	testtextrandom	5.75	6	1.544785952	5.75
ast118	testtextrandom	7.333333333	7	1.556997888	7.333333333
ast125	testtextrandom	6.214285714	5	3.555679561	6.25
ast131	testtextrandom	15.22222222	8.5	13.85876472	11.83333333
ast133	testtextrandom	14	13.5	6.196773354	14
ast134	testtextrandom	7.833333333	5.5	3.785938897	7.833333333
ast135	testtextrandom	NA	NA	NA	NA
ast136	testtextrandom	9.666666667	8	4.119429204	9.666666667
ast138	testtextrandom	16.15384615	15	5.698627815	16.15384615
ipt101	testpasstiles	14.60869565	11	8.768430618	10.69230769

ipt104	testpasstiles	23.55555556	22	5.85472269	23.55555556
ipt105	testpasstiles	10.94736842	7	7.884398689	9.083333333
ipt106	testpasstiles	22.92307692	13	38.12798958	24.08333333
ipt109	testpasstiles	24.58333333	21	12.09401304	24.58333333
ipt110	testpasstiles	19.61538462	12	28.80549271	11.66666667
ipt113	testpasstiles	9.923076923	7.5	13.12074107	11.21428571
ipt119	testpasstiles	13.2	8	13.7591528	14.07692308
ipt131	testpasstiles	37.83333333	34.5	15.63116545	35.44444444
ipt133	testpasstiles	21519.33333	16	74490.36161	21519.33333
ipt134	testpasstiles	23.76470588	23	7.395348299	23.83333333
ipt136	testpasstiles	12.13333333	11	3.502380143	11.33333333
ipt137	testpasstiles	20.46666667	18	7.707757379	19.38461538
ipt143	testpasstiles	25.33333333	11	43.37982854	27.75
ipt145	testpasstiles	24.23076923	23	5.847418891	23.58333333

SuccTestTimes.med	SuccfulTestTimes.sd	UnsuccfulTestTimes.mn	UnsuccTestTimes.med	UnsuccfulTestTimes.sd
4	14.85399023	17	17	NA
10	3.928854469	14	14	NA
7	2.048034288	8.5	8.5	6.363961031
4.5	2.065224326	5.5	4	4.23083916
3	1.222799287	NA	NA	NA
9	52.02643559	NA	NA	NA
7	2.256304299	NA	NA	NA
10.5	4.622081389	10.8	11	2.588435821
10	3.869069264	NA	NA	NA
6	1.544785952	NA	NA	NA
7	1.556997888	NA	NA	NA
5	3.768891807	6	6	2.828427125
8	7.732262204	22	9.5	20.94755356
13.5	6.196773354	NA	NA	NA
5.5	3.785938897	NA	NA	NA
NA	NA	NA	NA	NA
8	4.119429204	NA	NA	NA

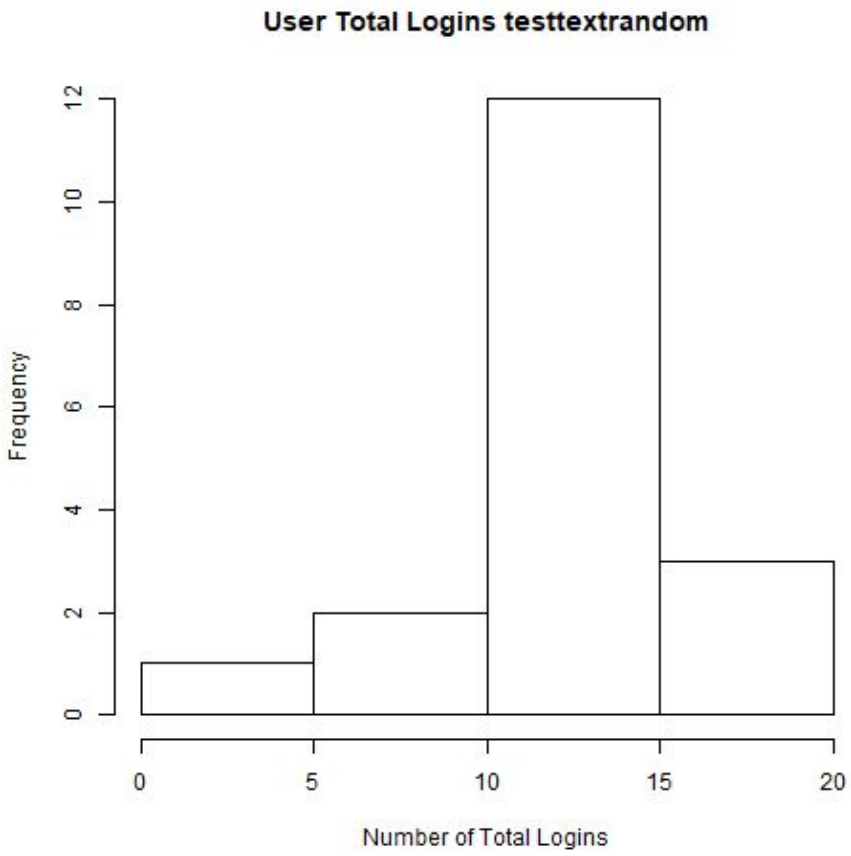
15	5.698627815	NA	NA	NA
10	1.652503928	19.7	17	11.5474865
22	5.85472269	NA	NA	NA
6.5	7.668807343	14.14285714	13	7.733661734
13.5	39.58295853	9	9	NA
21	12.09401304	NA	NA	NA
11.5	3.025147129	115	115	NA
6	17.73817514	8.416666667	10.5	3.848455023
9	14.64844439	7.5	7.5	0.7071067812
32	16.16408914	45	51	14
16	74490.36161	NA	NA	NA
21	8.472772792	23.6	24	4.615192304
11	3.200378765	15.33333333	14	3.214550254
18	5.8100267	27.5	27.5	17.67766953
10.5	48.52951304	15.66666667	14	6.658328118
22.5	5.599648257	32	32	NA

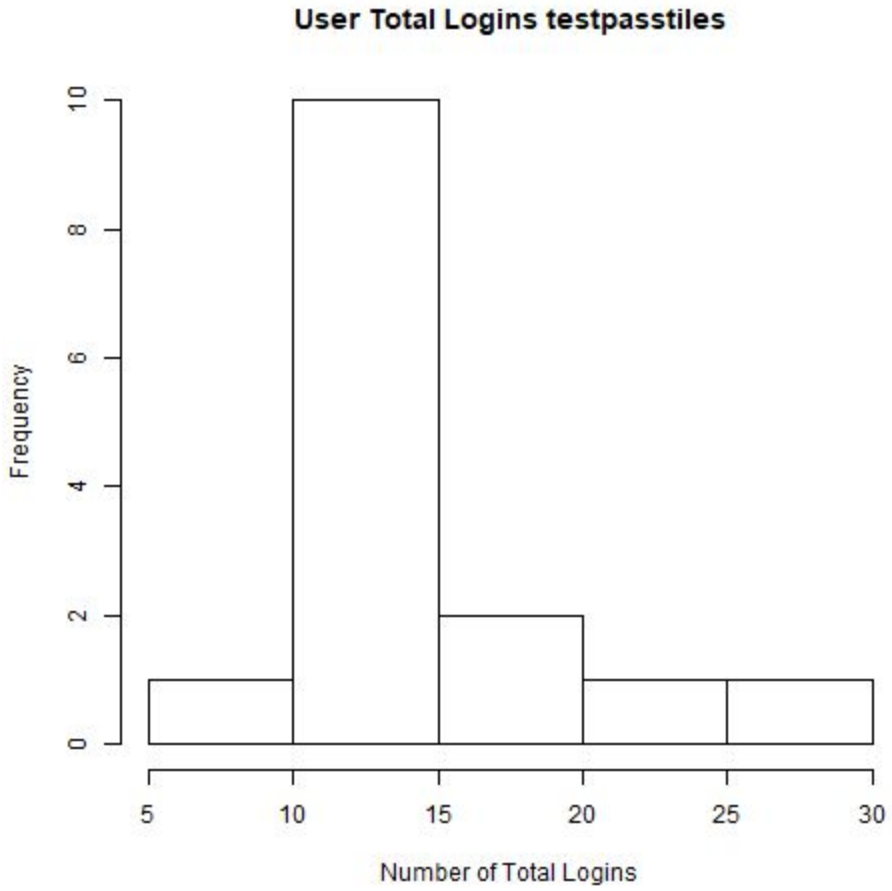
Graphs

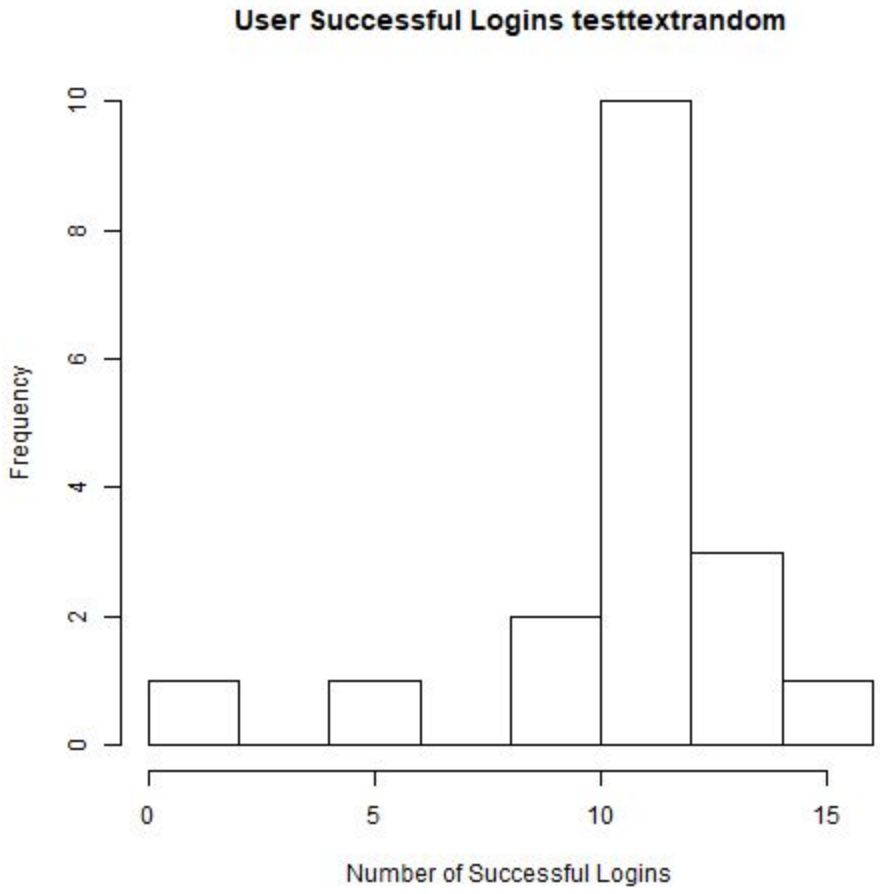
The following assortment of graphs was used to model the statistical relationships between each scheme and measures of their respective user login performance. Specifically, these graphs depict the relationship between scheme and total login time per user, and between scheme and total number of logins per user. As was the case with the descriptive statistics, testtextrandom refers to the Text21 scheme and testpasstiles refers to Imagept21.

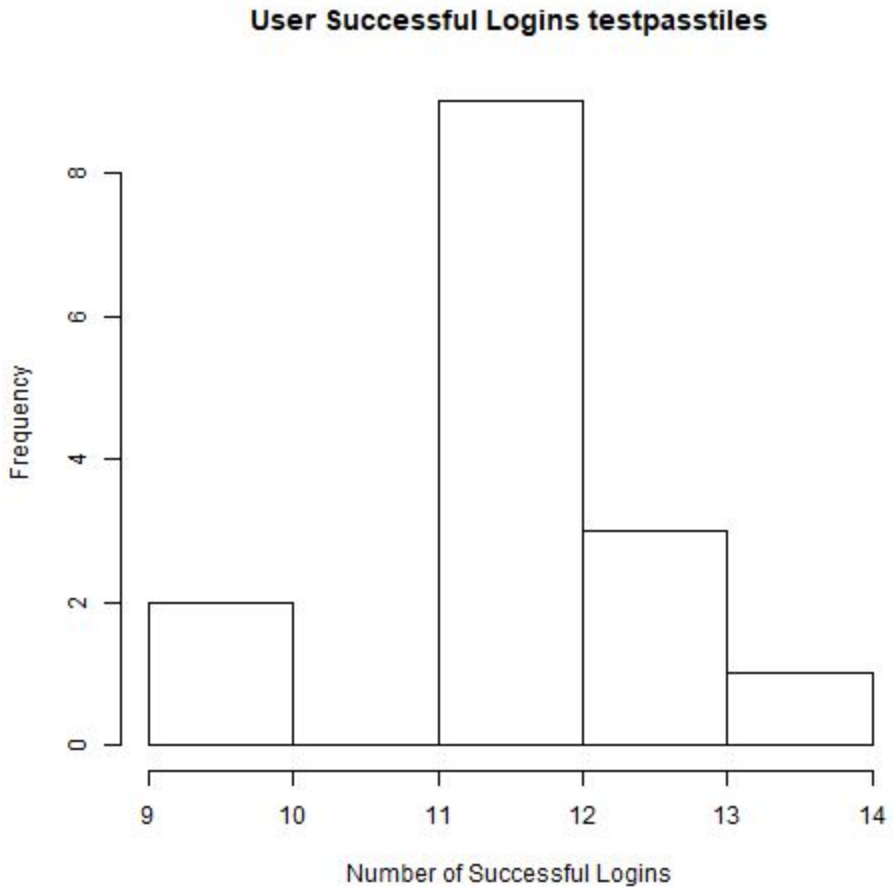
Total Number of Logins

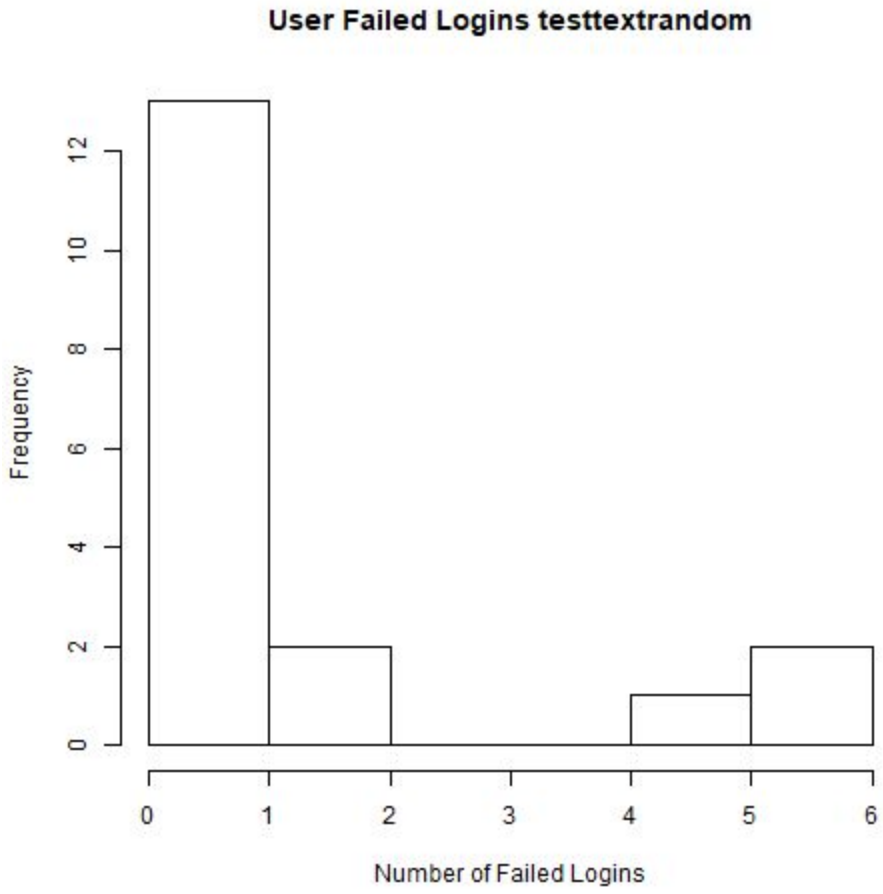
Histograms

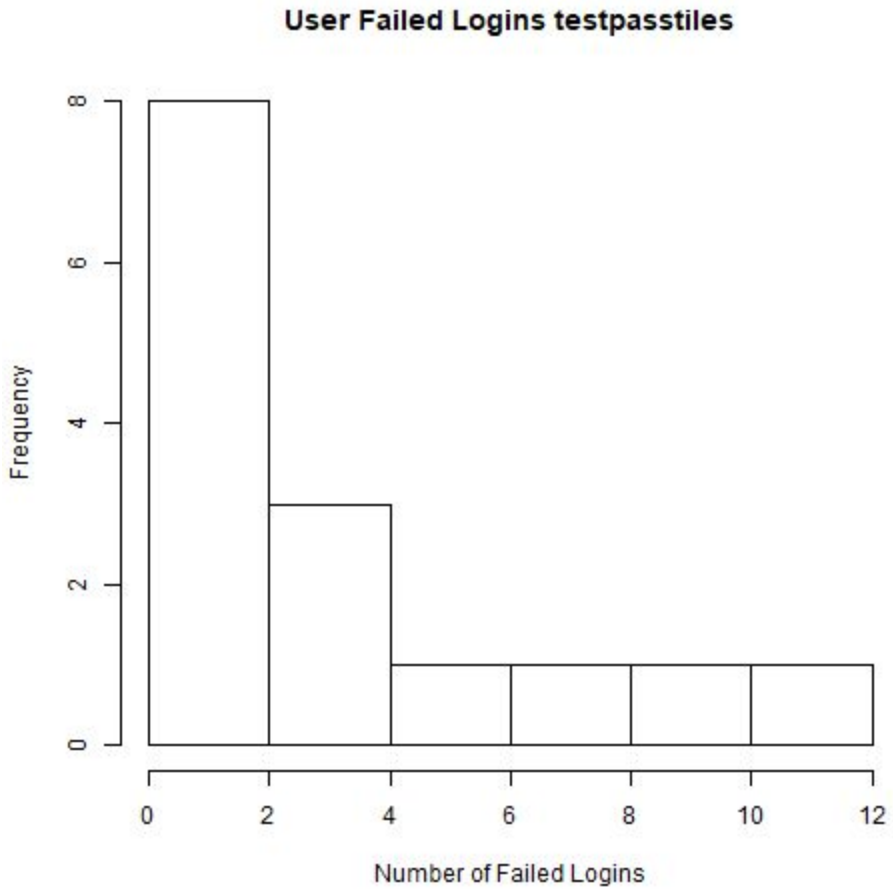



User Total Logins testpasstiles
Frequency
0
2
4
6
8
10
5
10
15
20
25
30
Number of Total Logins


User Successful Logins testtextrandom
Frequency
0
2
4
6
8
10
0
5
10
15
Number of Successful Logins

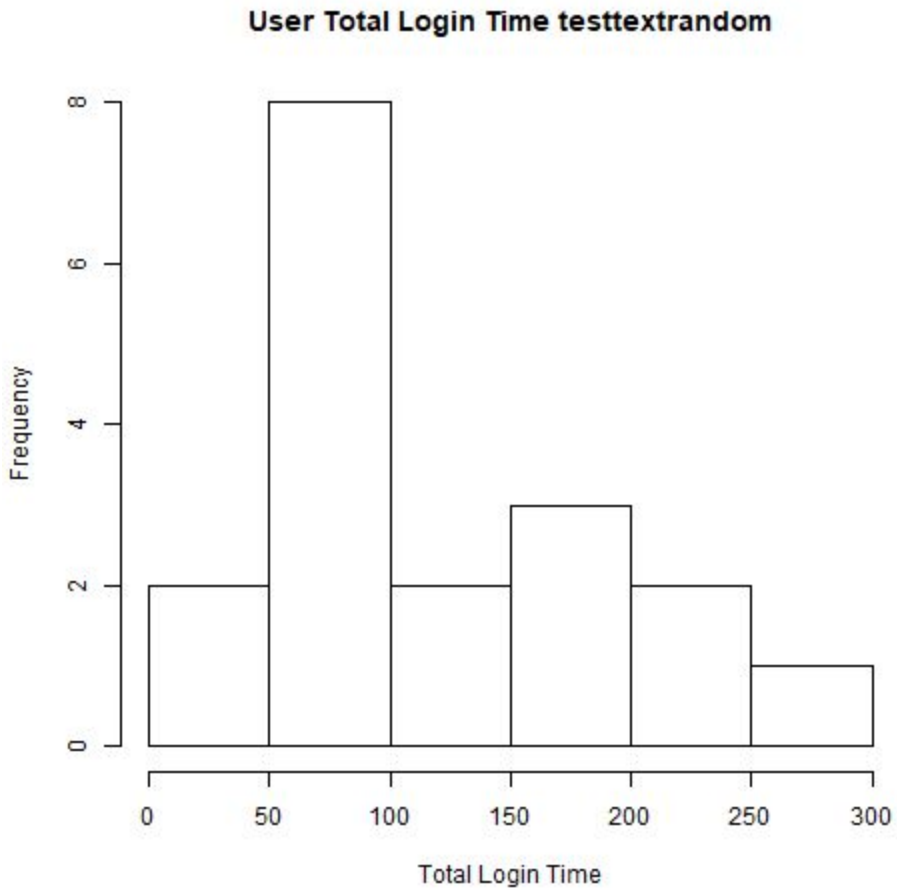

User Successful Logins testpasstiles
Frequency
0
2
4
6
8
9
10
11
12
13
14
Number of Successful Logins

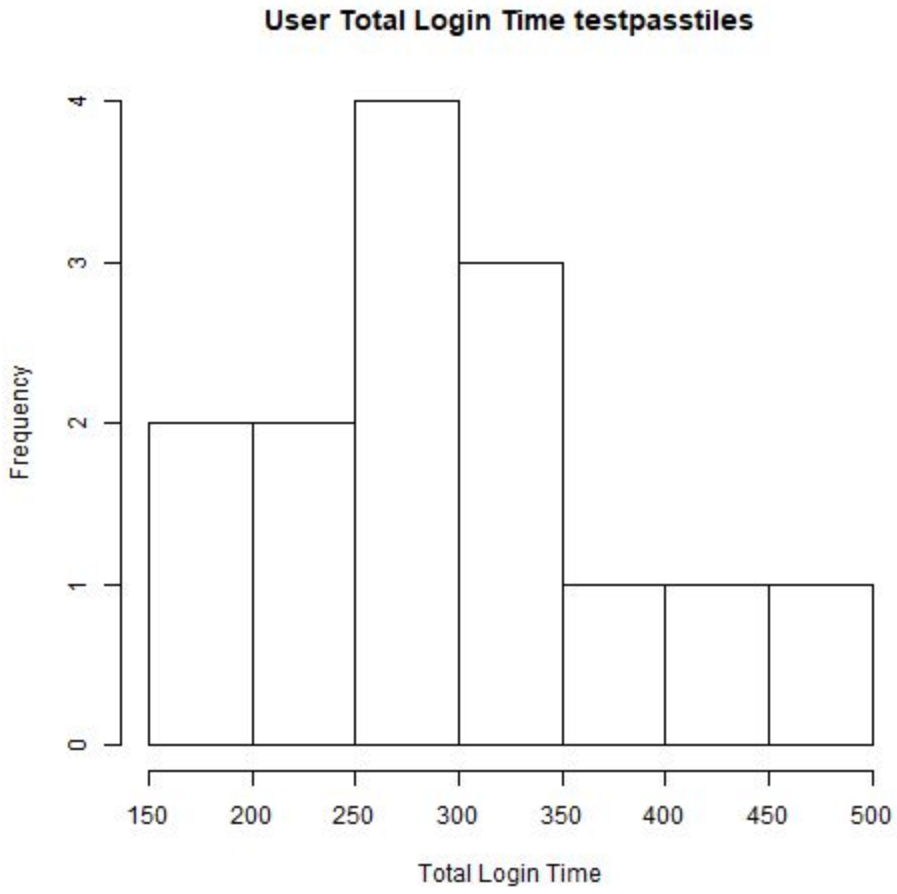

User Failed Logins testtextrandom
Frequency
0
2
4
6
8
10
12
0
1
2
3
4
5
6
Number of Failed Logins

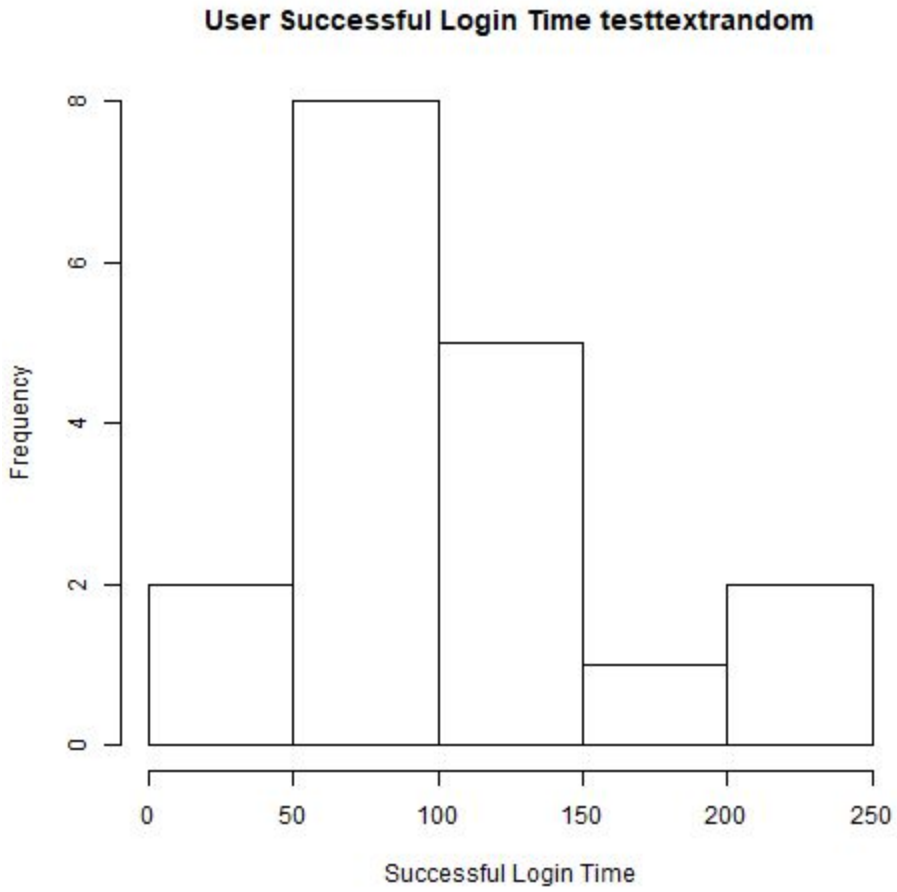


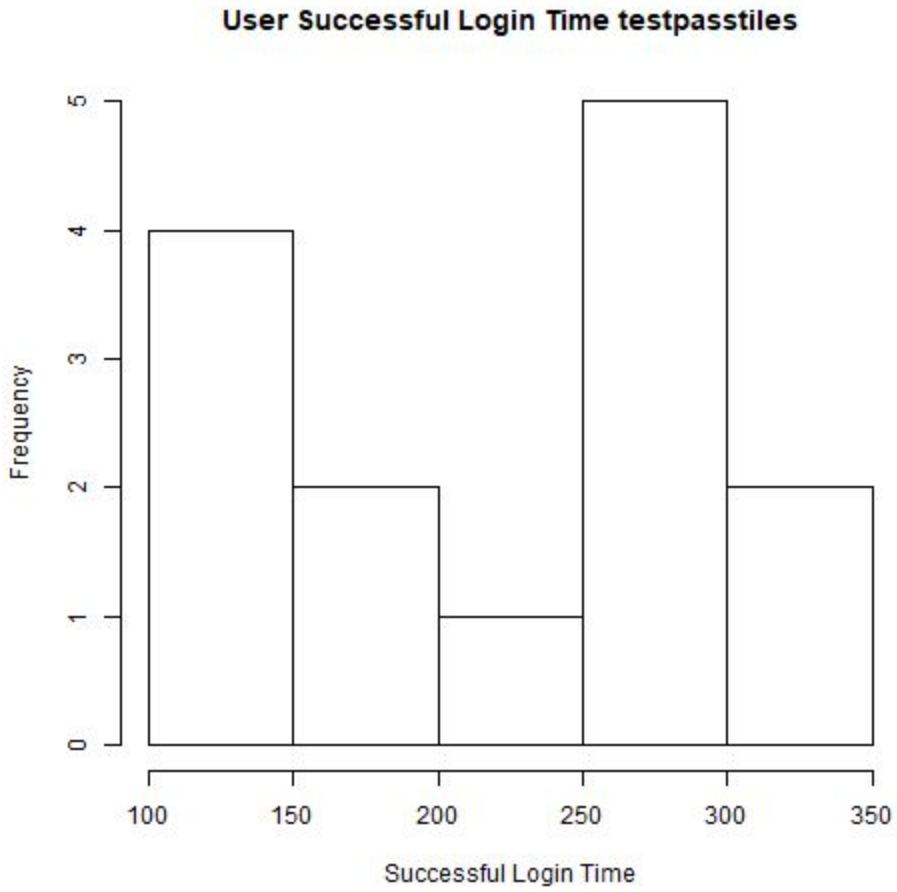
Login Times Per User

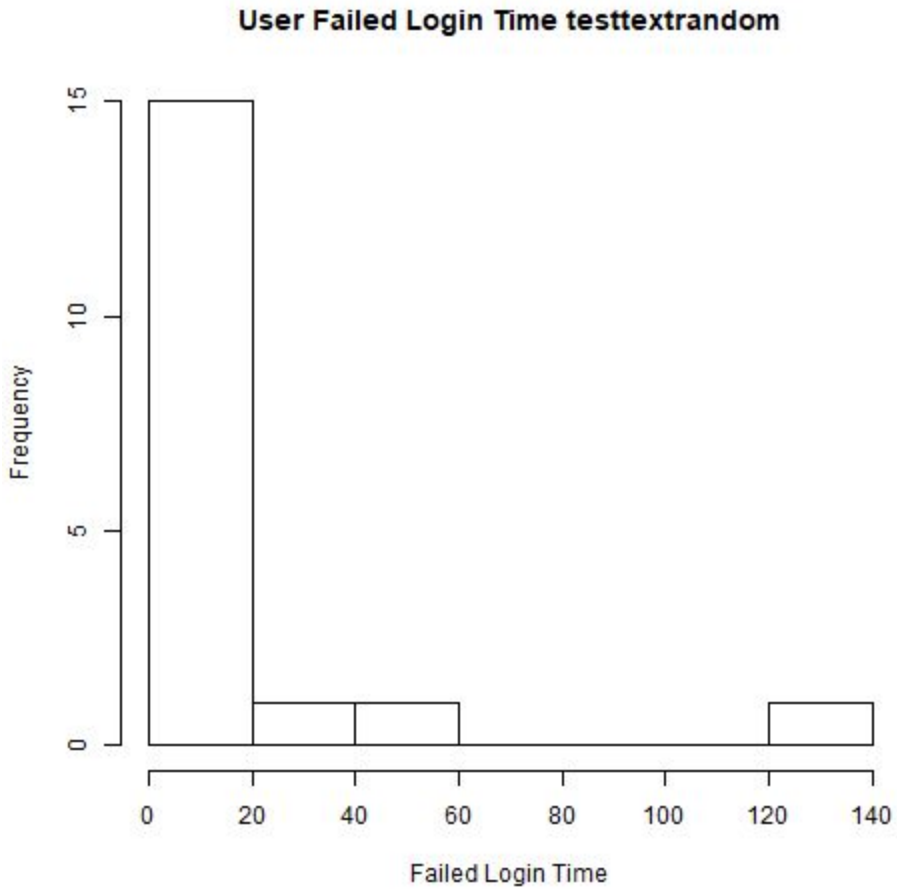
Histograms

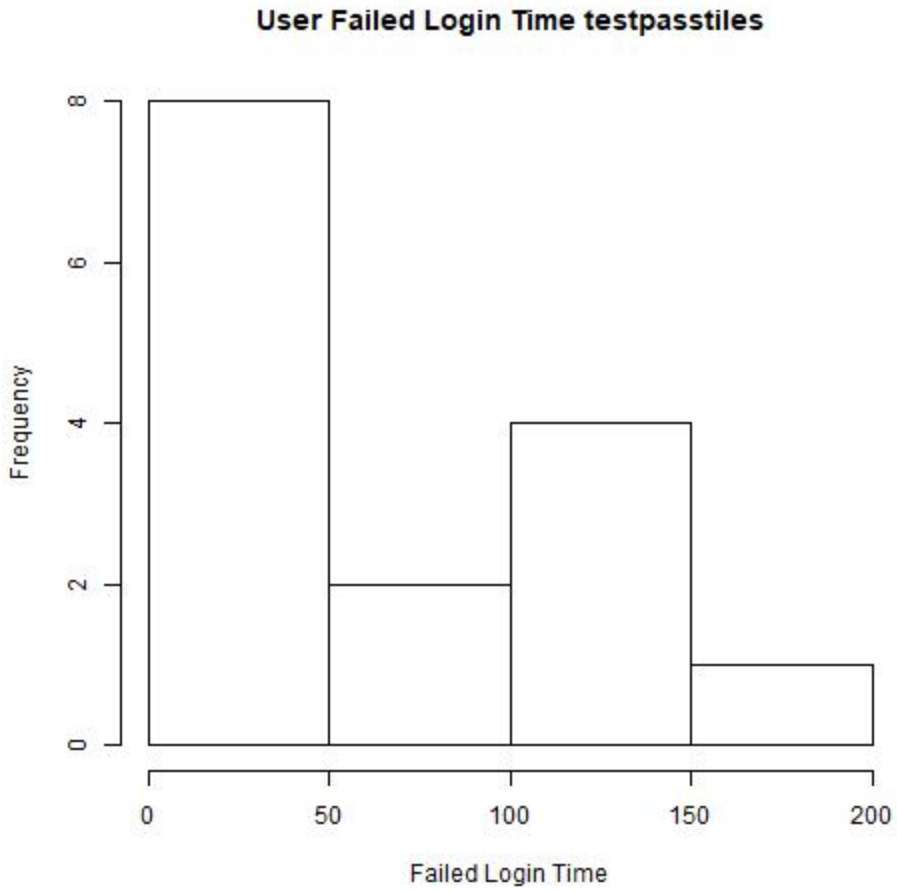

User Total Login Time testtextrandom
Frequency
0
2
4
6
8
0
50
100
150
200
250
300
Total Login Time


User Total Login Time testpasstiles
Frequency
0
1
2
3
4
150
200
250
300
350
400
450
500
Total Login Time

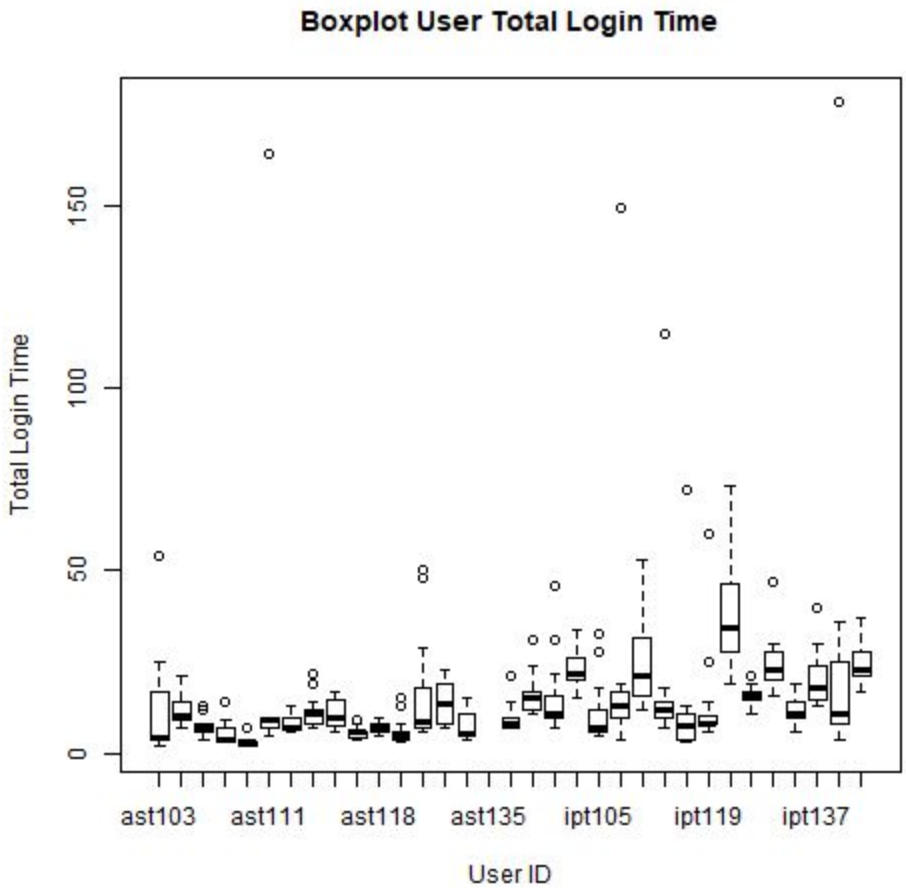

User Successful Login Time testtextrandom
Frequency
0
2
4
6
8
0
50
100
150
200
250
Successful Login Time

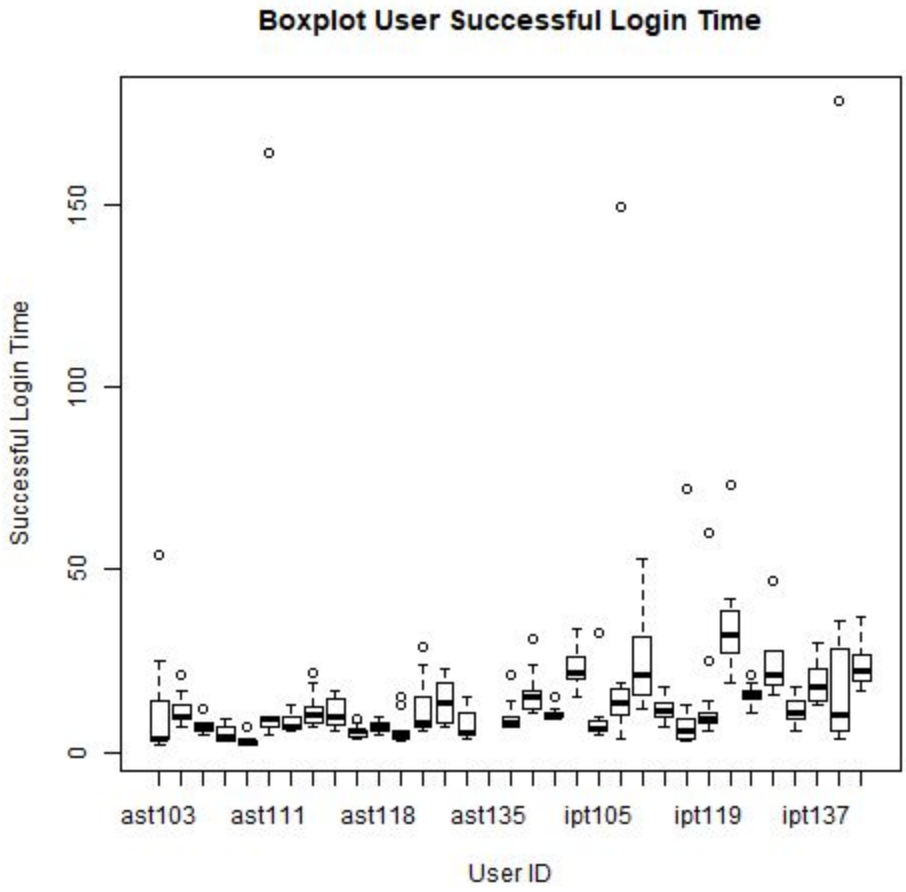

User Successful Login Time testpasstiles
Frequency
0
1
2
3
4
5
100
150
200
250
300
350
Successful Login Time

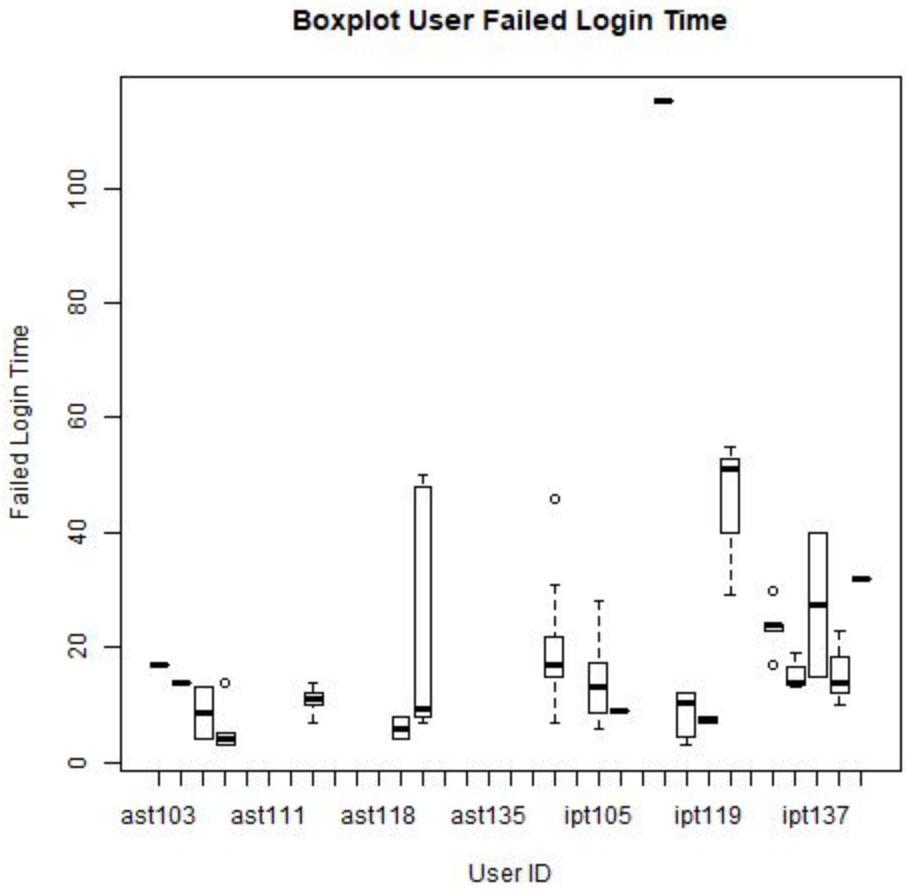

User Failed Login Time testtextrandom
Frequency
0
5
10
15
0
20
40
60
80
100
120
140
Failed Login Time

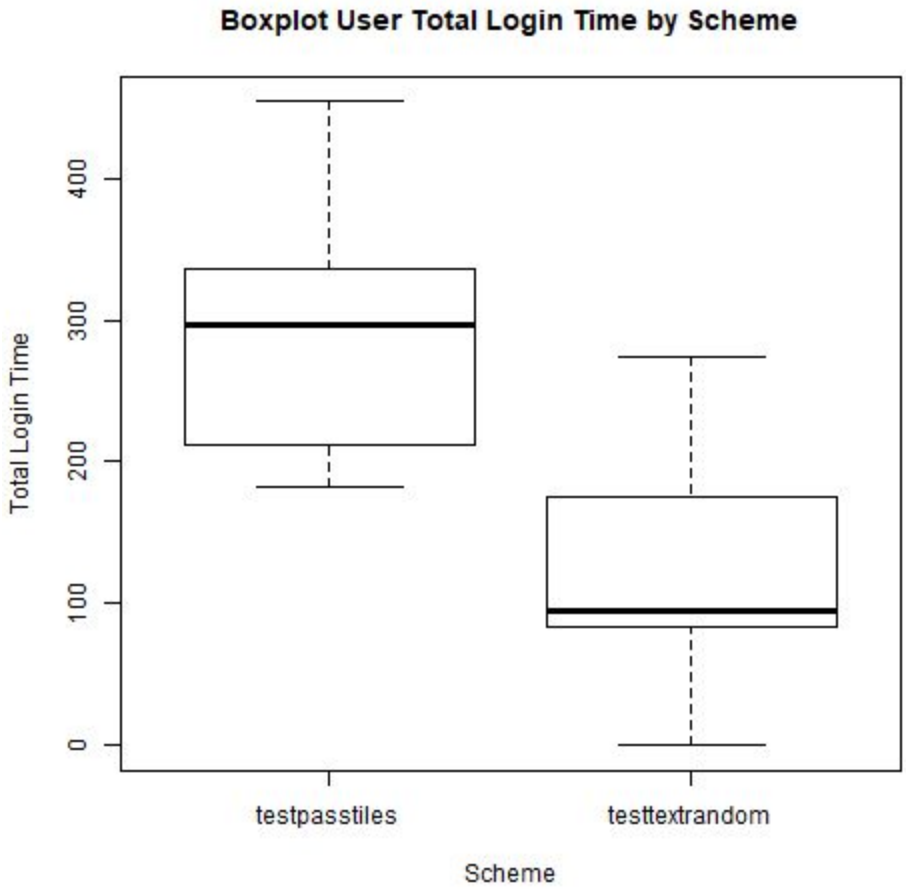

User Failed Login Time testpasstiles
Frequency
0
2
4
6
8
0
50
100
150
200
Failed Login Time

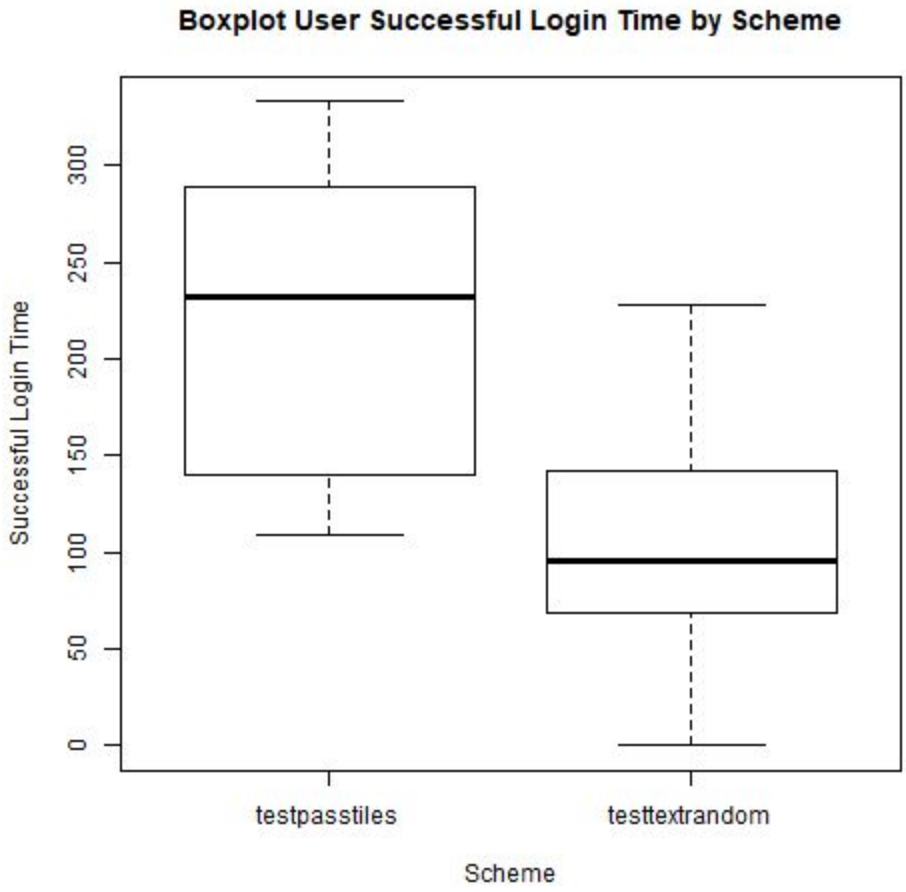
Box plots

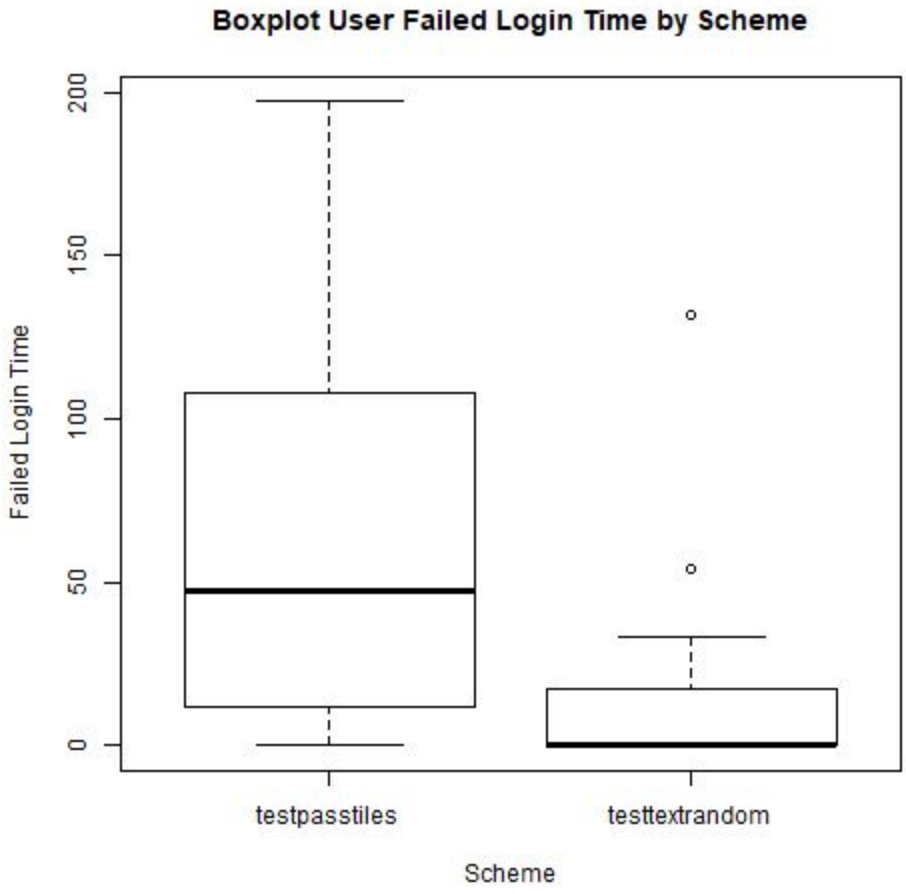

Boxplot User Total Login Time
Total Login Time
0
50
100
150
ast103
ast111
ast118
ast135
ipt105
ipt119
ipt137
User ID


Boxplot User Successful Login Time
Successful Login Time
0
50
100
150
ast103
ast111
ast118
ast135
ipt105
ipt119
ipt137
User ID


Boxplot User Failed Login Time
Failed Login Time
0
20
40
60
80
100
ast103
ast111
ast118
ast135
ipt105
ipt119
ipt137
User ID


Boxplot User Total Login Time by Scheme
Total Login Time
0
100
200
300
400
testpasstiles
testtextrandom
Scheme


Boxplot User Successful Login Time by Scheme
Successful Login Time
0
50
100
150
200
250
300
testpasstiles
testtextrandom
Scheme



Interpretation

Our interpretation of the graphs shown above are as follows: we think that in terms of usability, the Text21 password generation is the better choice over Imagept21. If you look at the graphs under Total Logins (successful logins vs freq.), you'll see that more users have successful logins using a textual password over a graphic, Ryan surmises that this may be related to 'memory chunking' that was mentioned earlier and the use of mnemonics. Also if you compare the failure frequency of total logins, more users tend to fail login with the graphical password, possibly due to complexity and abnormality for password input because at creation, it makes it harder to write into long term memory. However, the success that the graphical password has for logins can be attributed to some users having a stronger visual spatial memory because of the recognition factor that plays when the image is displayed in a grid. In regards to time,

the textual password will be faster (100ms, 1/10s) since access to the parts for the password are close at hand for the user whereas the graphical requires the user to move the cursor to specific regions. Now we do notice that the textual password does have a higher failure rate than the graphical possibly due to mistypes, brute forcing passwords from memory, and most of all, no recognition factor. The graphical has a lower failure rate because of the recall-recognition factor but has a longer input time (250ms, 1/4s) because of the need to use a mouse to hit the squares precisely for password input.

2: Design, Implementation, Statistical Inference

Scheme Rationale

The scheme that our group developed as a new authentication system allows users to associate their assigned password, a 4 character string such as “wjex”, to aspects of an image which itself is a mosaic of 4 randomly generated images merged together. The user can map each letter of the password to an aspect of each of the 4 images. The user, being encouraged to be as creative as possible in this process, forges strong memories that connect their password to the image, allowing greater recall. In the case that a user forgets their password, they can choose to receive a hint by being shown the image associated to their password. Displaying the image associated to the password when a user requests the hint does not in any way compromise the security of the password, as the images do not necessarily reveal anything about the password itself.

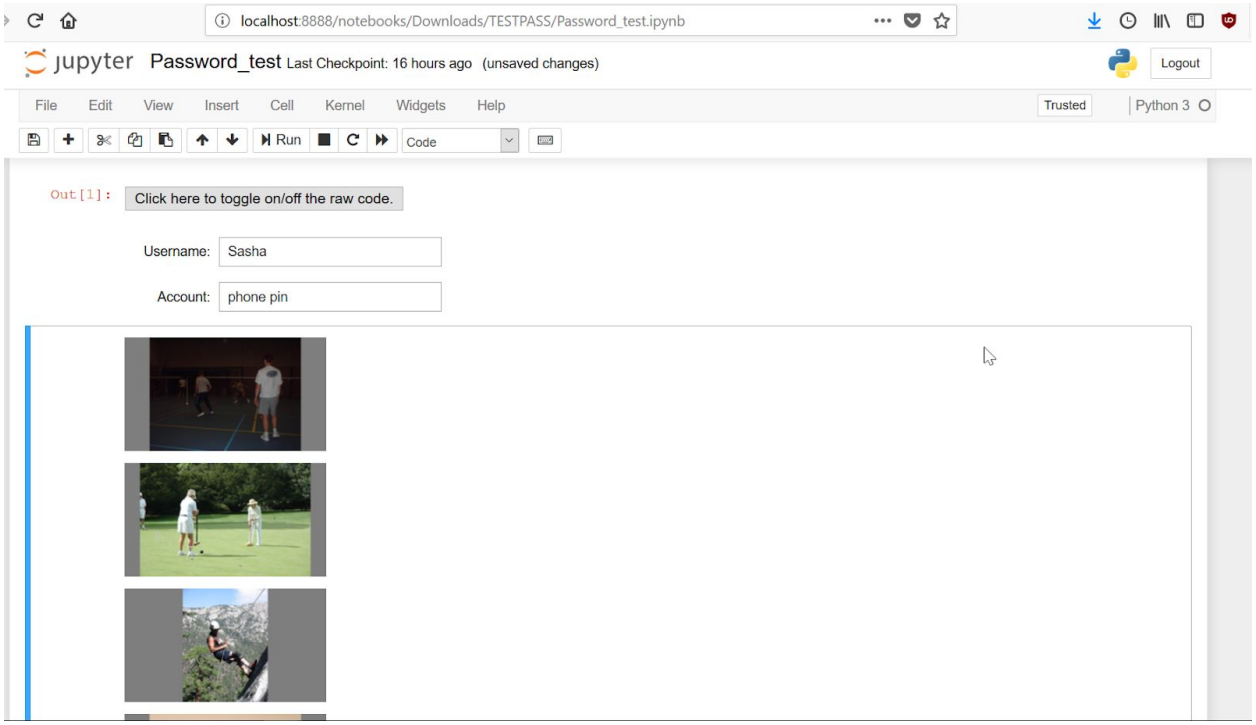
The authentication system we have proposed has a state space 4^26, as each randomly generated password, being of length 4, has 26 possible letters that can be used. We believe that this authentication system offers good usability for two reasons. Firstly, by providing the user a visual tool to help memorize their password, the user is able to impart their own creativity and personality to forge the connections between the password and the image. This process is analogous to the memory palace, better known as the Method of Loci, which has been shown to help recall by using visualizations to efficiently recall information. Secondly, this system uniquely is capable of providing users

hints without compromising the safety of the password, a feature that is rarely implemented amongst authentication systems.

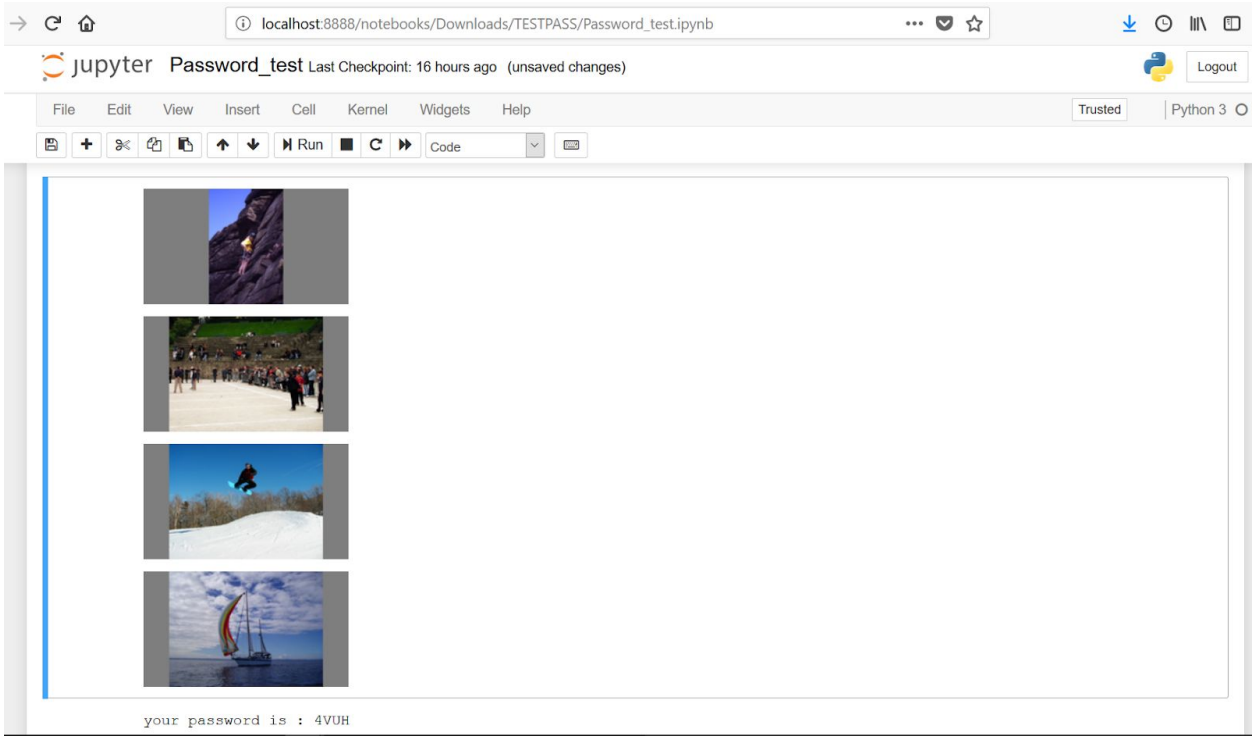
Scheme Implementation

Password Creation

1. Enter username and account



2. “Ctrl+Enter” Command to get new set of images for association with your password

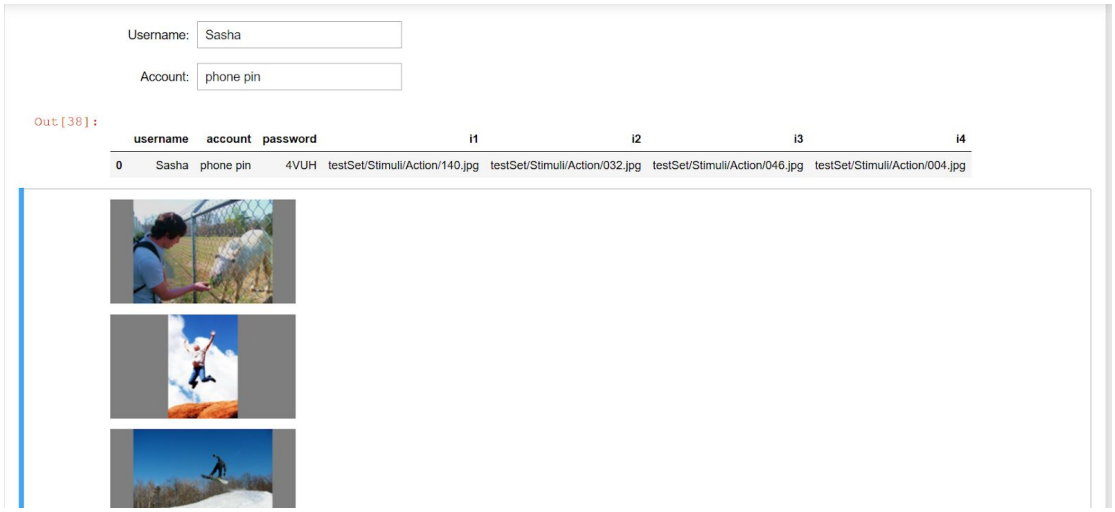


3.

>Type in username and account you want to check your password for

>Log for all usernames saved in system with their associated account and details

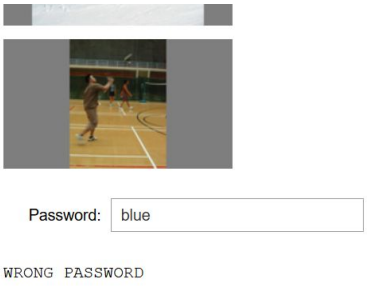
>Presented with associated pictures for username and account just typed in



Password Entry

4. > Prompted to type in password

> Message given when password is incorrect



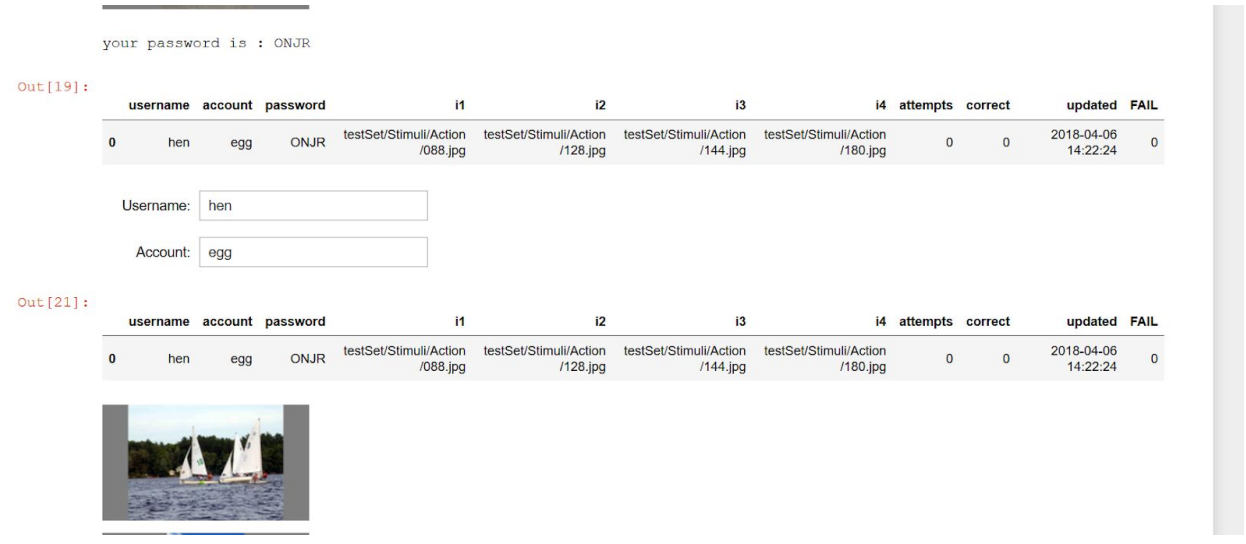
5. Message given when password is correct

Quantitative Testing Framework

Preface To Quantitative Testing Framework

It may be noticed that the results of the trial of our password scheme with ten individuals do not correlate to the format and output of password scheme program and the screenshots below. We would like to address this discrepancy by explaining that come the day of our demo, we experienced a failure of our code, resulting in the need to revert our project to a more primitive form of logging. As such, the logs associated to our password scheme on the day of testing deviate from the log system and its output that currently work and are attached in this submission. Thank you in advance for understanding the issue and our attempt to resolve it as such.

Screenshots of Testing Framework



```
your password is : ONJR
```

Out[19]:

	username	account	password	i1	i2	i3	i4	attempts	correct	updated	FAIL
0	hen	egg	ONJR	testSet/Stimuli/Action/088.jpg	testSet/Stimuli/Action/128.jpg	testSet/Stimuli/Action/144.jpg	testSet/Stimuli/Action/180.jpg	0	0	2018-04-06 14:22:24	0

Username: hen

Account: egg

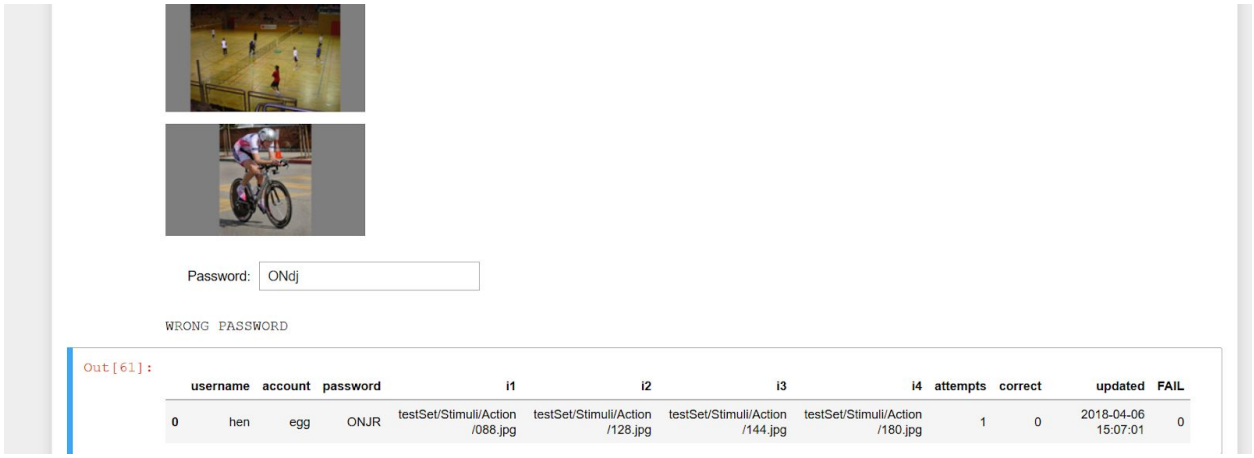
Out[21]:

	username	account	password	i1	i2	i3	i4	attempts	correct	updated	FAIL
0	hen	egg	ONJR	testSet/Stimuli/Action/088.jpg	testSet/Stimuli/Action/128.jpg	testSet/Stimuli/Action/144.jpg	testSet/Stimuli/Action/180.jpg	0	0	2018-04-06 14:22:24	0

Testing for Username: hen, Account: egg

Attempts:0 , Correct:0

FAIL ? No



Password: ONdj

WRONG PASSWORD

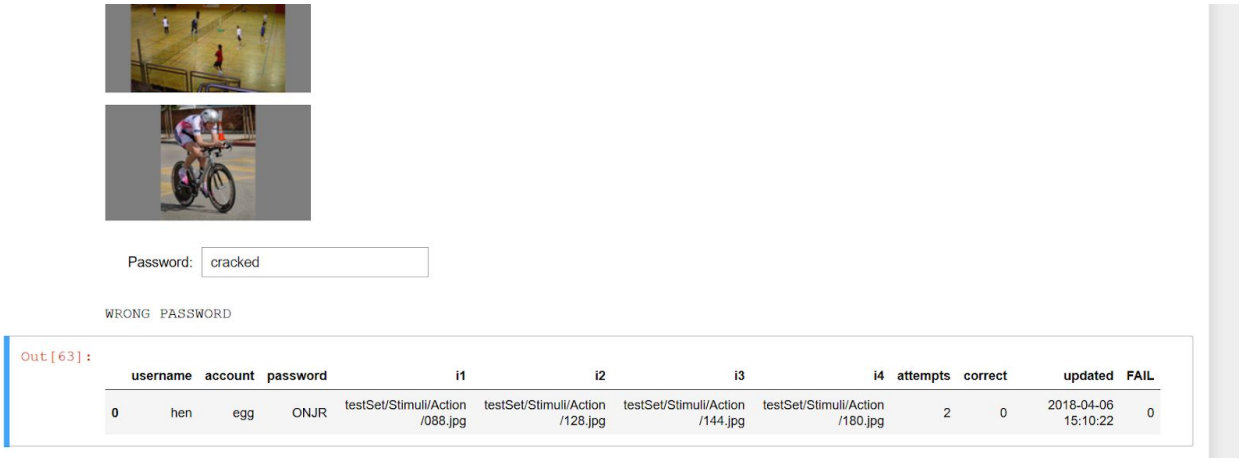
Out[61]:

	username	account	password	i1	i2	i3	i4	attempts	correct	updated	FAIL
0	hen	egg	ONJR	testSet/Stimuli/Action/088.jpg	testSet/Stimuli/Action/128.jpg	testSet/Stimuli/Action/144.jpg	testSet/Stimuli/Action/180.jpg	1	0	2018-04-06 15:07:01	0

Testing for Username: hen, Account: egg

Attempts:1 , Correct:0

FAIL ? No



Password: cracked

WRONG PASSWORD

Out[63]:

	username	account	password	i1	i2	i3	i4	attempts	correct	updated	FAIL
0	hen	egg	ONJR	testSet/Stimuli/Action/088.jpg	testSet/Stimuli/Action/128.jpg	testSet/Stimuli/Action/144.jpg	testSet/Stimuli/Action/180.jpg	2	0	2018-04-06 15:10:22	0

Testing for Username: hen, Account: egg

Attempts:2 , Correct:0

FAIL ? No

Password: fdj2

WRONG PASSWORD

Out[65]:

	username	account	password	i1	i2	i3	i4	attempts	correct	updated	FAIL
0	hen	egg	ONJR	testSet/Stimuli/Action/088.jpg	testSet/Stimuli/Action/128.jpg	testSet/Stimuli/Action/144.jpg	testSet/Stimuli/Action/180.jpg	3	0	2018-04-06 15:13:43	0

Testing for Username: hen, Account: egg

Attempts:2 , Correct:0

FAIL ? No

Password: chic

Unfortunately, you have exceeded the max attempts for this account, try another!

Out[83]:

	username	account	password	i1	i2	i3	i4	attempts	correct	updated	FAIL
0	hen	egg	ONJR	testSet/Stimuli/Action/088.jpg	testSet/Stimuli/Action/128.jpg	testSet/Stimuli/Action/144.jpg	testSet/Stimuli/Action/180.jpg	4	0	2018-04-06 15:20:10	1

Testing for Username: hen, Account: egg

Attempts:2 , Correct:0

FAIL ? Yes

When the user makes additional attempts after 3, the system registers this as a fail to the log and does not allow this.

Questionnaire

The original survey can be found through the following link to a limesurvey Questionnaire: https://hotsoft.carleton.ca/comp3008limesurvey/index.php/676193?token=12345678&lang=en

Section A: Image Based Password Perception

10-20 likert scale questions

A1. **The instructions for how to use our password memorization tool was clear**

(1 = Strongly Disagree) -(3= Neutral) -(5 = Strongly Agree)

1 ☐
2 ☐
3 ☐
4 ☐
5 ☐

A2. **Did you find it easy to use the provided images to help memorize the assigned passwords?**

(1 = Strongly Disagree) -(3= Neutral) -(5 = Strongly Agree)

1 ☐
2 ☐
3 ☐
4 ☐
5 ☐

A3. **The experience of trying to memorize three passwords was mentally taxing**

(1 = Strongly Disagree) -(3= Neutral) -(5 = Strongly Agree)

1 ☐
2 ☐
3 ☐
4 ☐
5 ☐

A4. **Memorizing the middle password was more difficult than memorizing the first and third password.**

(1 = Strongly Disagree) -(3= Neutral) -(5 = Strongly Agree)

1 ☐
2 ☐
3 ☐
4 ☐
5 ☐

A5. **You tend to find it difficult to remember passwords in general**

(1 = Strongly Disagree) -(3= Neutral) -(5 = Strongly Agree)

1 ☐
2 ☐
3 ☐
4 ☐
5 ☐

A6. **When associating your password to the image, you felt creatively capable to come up with unique and memorable connections between the two.**

(1 = Strongly Disagree) -(3= Neutral) -(5 = Strongly Agree)

1 ☐
2 ☐
3 ☐
4 ☐
5 ☐

A7. **When choosing an image to associate to a password, you had to request a new image:**

1= once new images

2= twice new images

3= three new images

4= four new images

5 = ZERO requests for new images.

1 ☐
2 ☐
3 ☐
4 ☐
5 ☐

A8. **You believe that memorizing passwords with pictures is a bad approach in general:**

(1 = Strongly Disagree) -(3= Neutral) -(5 = Strongly Agree)

1 ☐
2 ☐
3 ☐
4 ☐
5 ☐

A9. **Please pick the number of passwords you remember for the various computer based tools and services that you use.**

1 ☐
2 ☐
3 ☐
4 ☐
5 ☐

A10. **If you were required to memorize three randomly assigned passwords, as you were in this experiment, you would use the image based memorization system just presented now.**

(1 = Strongly Disagree) -(3= Neutral) -(5 = Strongly Agree)

1 ☐
2 ☐
3 ☐
4 ☐
5 ☐

Thanks for taking this survey and for participating

Comparison with Text21

In comparison with Text21, we can agree that users feel comfortable with understanding and using the password scheme instructions. In relation to Imagept21's implementation, users believe that having some kind of association with the password makes it more memorable however it is very dependent on the image being used during password creation that allows a permeable link to be made in memory which would explain why users have the need to request for new images in our questionnaire. Similar to Text21's textual password, we use keyboard input for a faster login attempt than using a mouse input to allow users to quickly try another password should they fail previously. This allows them to systematically go through their passwords that come to mind quickly and efficiently so that way they don't spend a lot of time trying to guess. For when they do forget their password, we provide a visual cue similar to Imagept21's tiles to allow the user to figure out the association they've made between their password and the images presented.

What's interesting is that we have a normal distribution for the people that claim to remember their passwords however they also state that can remember passwords used for multiple services. This could imply that some users use a variation of an existing password possibly if the existing doesn't fit the scheme of the password system. For instance a password scheme that's all text, I could use "server" however for another that requires at least one of each upper, lower, and numeric characters I would use "S3rver" to minimize the amount of change I would make to my 'master' password.

Based on our observations, we argue that the medium of images offers unique strengths that our password scheme leverages making it in some respects more effective than Text21 and Imagept21. In our implementation, we took the two strongest features from each: Text21's fast input method and textual format, and Imagept21's visual cueing to the user to allow them to recognize the images presented from creation and recall the password associated. As to whether end-users will want to use this kind of scheme over the normal is hard to say, mostly because there's more benefits to users with a stronger visual memory because once they see the password hint then they can make that association to the right password whereas someone else may be presented the hint but not know it's association at all and would rather have a hint such as the starting letter or

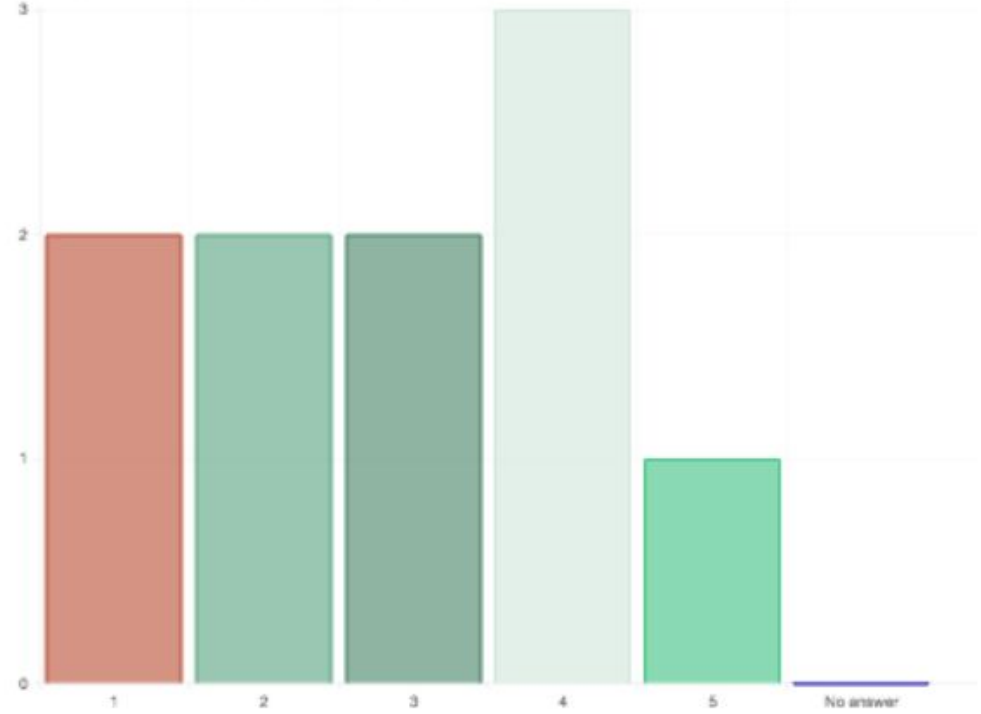
even knowing the password constraints itself but obviously has a negative effect in terms of security. With that being said, primitive features from an image are easier to foveate on and process into episodic memory which can then be later recalled than retrieving from semantic memory without any kind of strong cue like a recovery email or password that's currently implemented on existing textual password systems like email and 2-step verification.

Interpretation from Questionnaire **(Comparison w/ Text21 & Imagept21)**:

- Users felt comfortable with the instructions (**Similarity**)
- Majority of users found scheme to be easy to use with provided images (**Difference**)
- Normal distribution for remembering the password (**Difference, Irrelevant**)
- Most users needed a new images to better associate the images with password
- Most users felt capable of creating a memorable connection between the image and the password, somewhat contradicts the note above. (**Similarity**)
- Users believe that memorizing passwords with images is a good approach (**Similarity**)
- Users remember the passwords for multiple services, but are those passwords the same or variations of one another?

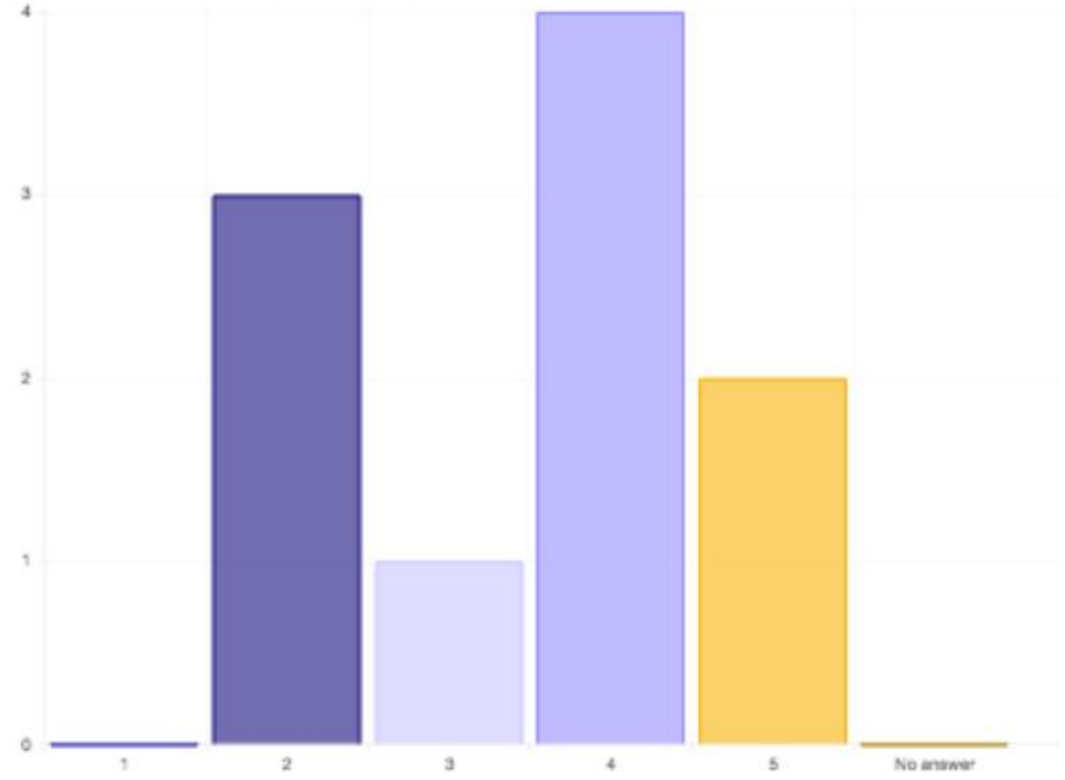
The experience of trying to memorize three passwords was mentally taxing (1 = Strongly Disagree) -(3= Neutral) -(5 = Strongly Agree)

Arithmetic mean 2.9 Standard deviation 1.37



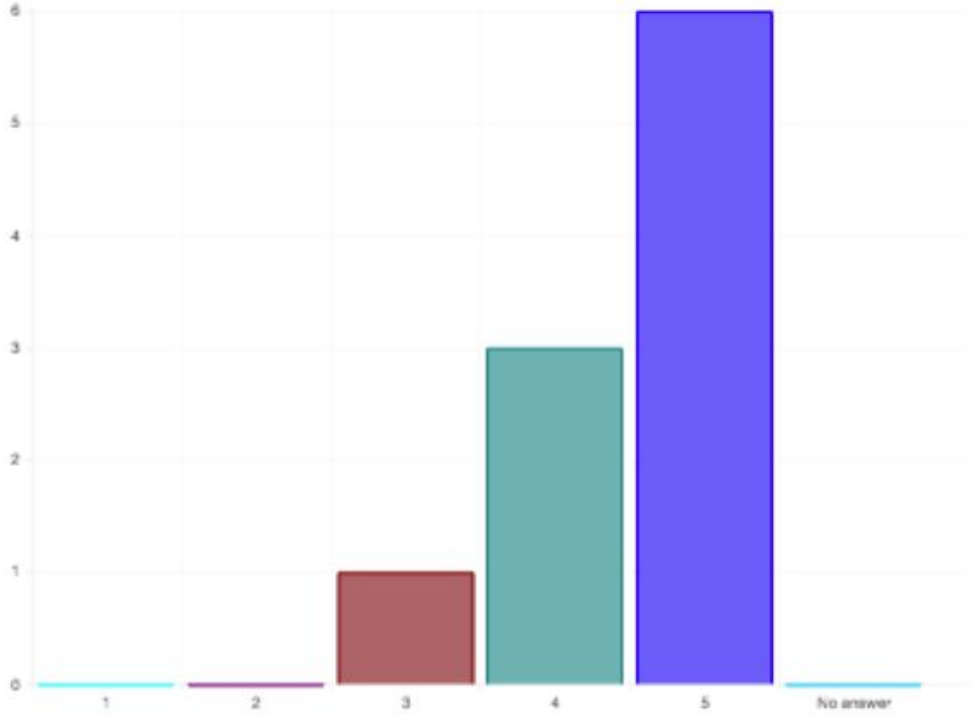
When associating your password to the image, you felt creatively capable to come up with unique and memorable connections between the two. (1 = Strongly Disagree) -(3= Neutral) -(5 = Strongly Agree)

Arithmetic mean 3.5 Standard deviation 1.18



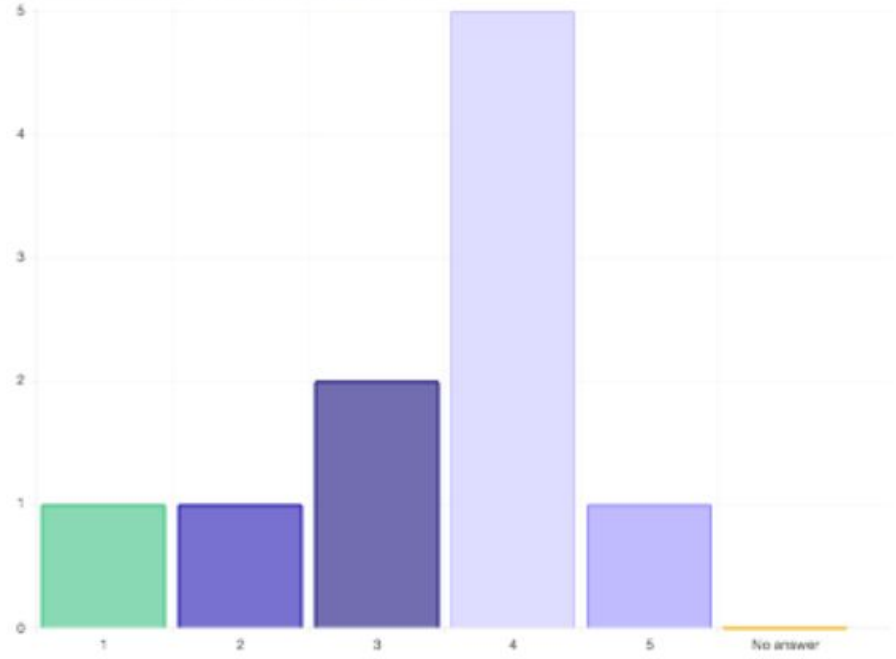
Please pick the number of passwords you remember for the various computer based tools and services that you use.

Arithmetic mean 4.5 Standard deviation 0.71



Did you find it easy to use the provided images to help memorize the assigned passwords? (1 = Strongly Disagree) -(3= Neutral) - (5 = Strongly Agree)

Arithmetic mean 3.4 Standard deviation 1.17



3: Appendix

Consent Forms

Carleton UNIVERSITY
Canada's Capital University

Carleton University, School of Computer Science
COMP3008: Human-Computer Interaction, Winter, 2018

Interaction Design Project User Consent Form

Instructor: Prof. Robert Biddle
Office: HP5169, Tel. Ext. 6317, Email: robert.biddle@carleton.ca

COMP3008 Student Names:

Ryan Samaroo, Heela Bangash, Frerik Drumm, Sammy Diamantstein, Brandon Esford

---

Note: This project was reviewed by the Carleton University Research Ethics Board (CUREB-B), which provided clearance to carry out the research: (Clearance #105985).

If you have any ethical concerns with the study, please contact Dr. Andy Adler, Chair, Carleton University Research Ethics Board-B (by phone at 613-520-2600 ext. 4085 or via email at ethics@carleton.ca

Study Purpose: This project is to enable students in COMP3008 to experience working with potential users to better understand testing of software using quantitative measures and analysis. Working with potential users is considered best practice in the design of interactive computer systems, and is identified in international standards such as ISO 9241-210:2010 — Human-centred design for interactive systems. Part of the process is first obtaining informed consent from prospective participants, and that is the reason for this form.

Study Procedure: In the project, the proposed system is a kind of password system, where users will be asked to use the system, remember some random passwords, and then try to use them to simulate login to a system. At no time will you be asked for any of your real passwords on any real systems. You will also be asked to fill out a questionnaire about your perceptions of the software and related issues.

Risks, Benefits, Compensation: We are not aware of any risks associated with this study. The benefits are that COMP3008 students gain experience in this aspect of Human Computer Interaction Design, and that you may gain some insight about the processes involved. There will be no financial compensation for your participation in the study.

Consent and Withdrawal: We require your consent before you can participate in the student, which you may indicate by signing your initials in the space provided below. You may choose to withdraw from the study at any time and without explanation, in which case any collected data will be discarded.

Anonymity and Confidentiality: The study involves gaining better general understanding of how students plan their degree programs, but does not involve asking you any specific personal information, nor any specific details of your degree or courses. We do not record or even ask your full name. We will not record or divulge any personal information about you.

By signing with your initials below, you consent to participate in the study.

Initials: B. E

Date: Apr. 03 2018

Carleton University, School of Computer Science
COMP3008: Human-Computer Interaction, Winter, 2018

Interaction Design Project User Consent Form

Instructor: Prof. Robert Biddle
Office: HP5169, Tel. Ext. 6317, Email: robert.biddle@carleton.ca

COMP3008 Student Names:

Ryan Samroo, Heela Bangash, Frerik Drum, Sammy Diamantstein, Brandon Esford

---

Note: This project was reviewed by the Carleton University Research Ethics Board (CUREB-B), which provided clearance to carry out the research: (Clearance #105985).

If you have any ethical concerns with the study, please contact Dr. Andy Adler, Chair, Carleton University Research Ethics Board-B (by phone at 613-520-2600 ext. 4085 or via email at ethics@carleton.ca

Study Purpose: This project is to enable students in COMP3008 to experience working with potential users to better understand testing of software using quantitative measures and analysis. Working with potential users is considered best practice in the design of interactive computer systems, and is identified in international standards such as ISO 9241-210:2010 — Human-centred design for interactive systems. Part of the process is first obtaining informed consent from prospective participants, and that is the reason for this form.

Study Procedure: In the project, the proposed system is a kind of password system, where users will be asked to use the system, remember some random passwords, and then try to use them to simulate login to a system. At no time will you be asked for any of your real passwords on any real systems. You will also be asked to fill out a questionnaire about your perceptions of the software and related issues.

Risks, Benefits, Compensation: We are not aware of any risks associated with this study. The benefits are that COMP3008 students gain experience in this aspect of Human Computer Interaction Design, and that you may gain some insight about the processes involved. There will be no financial compensation for your participation in the study.

Consent and Withdrawal: We require your consent before you can participate in the student, which you may indicate by signing your initials in the space provided below. You may choose to withdraw from the study at any time and without explanation, in which case any collected data will be discarded.

Anonymity and Confidentiality: The study involves gaining better general understanding of how students plan their degree programs, but does not involve asking you any specific personal information, nor any specific details of your degree or courses. We do not record or even ask your full name. We will not record or divulge any personal information about you.

By signing with your initials below, you consent to participate in the study.

Initials:  Date: 03/04/2018

Carleton University, School of Computer Science
COMP3008: Human-Computer Interaction, Winter, 2018

Interaction Design Project User Consent Form

Instructor: Prof. Robert Biddle
Office: HP5169, Tel. Ext. 6317, Email: robert.biddle@carleton.ca

COMP3008 Student Names:

Group registered: Brett Olsen, Ryan Samaroo, Sam Diamenstein, Heela Bagegh

Note: This project was reviewed by the Carleton University Research Ethics Board (CUREB-B), which provided clearance to carry out the research: (Clearance #105985).

If you have any ethical concerns with the study, please contact Dr. Andy Adler, Chair, Carleton University Research Ethics Board-B (by phone at 613-520-2600 ext. 4085 or via email at ethics@carleton.ca

Study Purpose: This project is to enable students in COMP3008 to experience working with potential users to better understand testing of software using quantitative measures and analysis. Working with potential users is considered best practice in the design of interactive computer systems, and is identified in international standards such as ISO 9241-210:2010 — Human-centred design for interactive systems. Part of the process is first obtaining informed consent from prospective participants, and that is the reason for this form.

Study Procedure: In the project, the proposed system is a kind of password system, where users will be asked to use the system, remember some random passwords, and then try to use them to simulate login to a system. At no time will you be asked for any of your real passwords on any real systems. You will also be asked to fill out a questionnaire about your perceptions of the software and related issues.

Risks, Benefits, Compensation: We are not aware of any risks associated with this study. The benefits are that COMP3008 students gain experience in this aspect of Human Computer Interaction Design, and that you may gain some insight about the processes involved. There will be no financial compensation for your participation in the study.

Consent and Withdrawal: We require your consent before you can participate in the student, which you may indicate by signing your initials in the space provided below. You may choose to withdraw from the study at any time and without explanation, in which case any collected data will be discarded.

Anonymity and Confidentiality: The study involves gaining better general understanding of how students plan their degree programs, but does not involve asking you any specific personal information, nor any specific details of your degree or courses. We do not record or even ask your full name. We will not record or divulge any personal information about you.

By signing with your initials below, you consent to participate in the study.

Initials: BO

Date: April 3/18

Carleton UNIVERSITY

Carleton University, School of Computer Science
COMP3008: Human-Computer Interaction, Winter, 2018
Interaction Design Project User Consent Form
Instructor: Prof. Robert Biddle
Office: HP5169, Tel. Ext. 6317, Email: robert.biddle@carleton.ca

COMP3008 Student Names:

Braden Esford, Heela Bagosh, Ryan Santos, Frank Orumm, Sanya Digiacomo, ...

Note: This project was reviewed by the Carleton University Research Ethics Board (CUREB-B), which provided clearance to carry out the research: (Clearance #105985).

If you have any ethical concerns with the study, please contact Dr. Andy Adler, Chair, Carleton University Research Ethics Board-B (by phone at 613-520-2600 ext. 4085 or via email at ethics@carleton.ca

Study Purpose: This project is to enable students in COMP3008 to experience working with potential users to better understand testing of software using quantitative measures and analysis. Working with potential users is considered best practice in the design of interactive computer systems, and is identified in international standards such as ISO 9241-210:2010 — Human-centred design for interactive systems. Part of the process is first obtaining informed consent from prospective participants, and that is the reason for this form.

Study Procedure: In the project, the proposed system is a kind of password system, where users will be asked to use the system, remember some random passwords, and then try to use them to simulate login to a system. At no time will you be asked for any of your real passwords on any real systems. You will also be asked to fill out a questionnaire about your perceptions of the software and related issues.

Risks, Benefits, Compensation: We are not aware of any risks associated with this study. The benefits are that COMP3008 students gain experience in this aspect of Human Computer Interaction Design, and that you may gain some insight about the processes involved. There will be no financial compensation for your participation in the study.

Consent and Withdrawal: We require your consent before you can participate in the student, which you may indicate by signing your initials in the space provided below. You may choose to withdraw from the study at any time and without explanation, in which case any collected data will be discarded.

Anonymity and Confidentiality: The study involves gaining better general understanding of how students plan their degree programs, but does not involve asking you any specific personal information, nor any specific details of your degree or courses. We do not record or even ask your full name. We will not record or divulge any personal information about you.

By signing with your initials below, you consent to participate in the study.

Initials: GW   Date: Apr 3, 2018

Carleton UNIVERSITY

Carleton University, School of Computer Science
COMP3008: Human-Computer Interaction, Winter, 2018

Interaction Design Project User Consent Form

Instructor: Prof. Robert Biddle
Office: HP5169, Tel. Ext. 6317, Email: robert.biddle@carleton.ca

COMP3008 Student Names:
Heela Bagosh
Frenie Orumm ~~Laura~~ Ryan Sanaroo, Sam Dianovski, Brandon Bedford

Note: This project was reviewed by the Carleton University Research Ethics Board (CUREB-B), which provided clearance to carry out the research: (Clearance #105985).

If you have any ethical concerns with the study, please contact Dr. Andy Adler, Chair, Carleton University Research Ethics Board-B (by phone at 613-520-2600 ext. 4085 or via email at ethics@carleton.ca

Study Purpose: This project is to enable students in COMP3008 to experience working with potential users to better understand testing of software using quantitative measures and analysis. Working with potential users is considered best practice in the design of interactive computer systems, and is identified in international standards such as ISO 9241-210:2010 — Human-centred design for interactive systems. Part of the process is first obtaining informed consent from prospective participants, and that is the reason for this form.

Study Procedure: In the project, the proposed system is a kind of password system, where users will be asked to use the system, remember some random passwords, and then try to use them to simulate login to a system. At no time will you be asked for any of your real passwords on any real systems. You will also be asked to fill out a questionnaire about your perceptions of the software and related issues.

Risks, Benefits, Compensation: We are not aware of any risks associated with this study. The benefits are that COMP3008 students gain experience in this aspect of Human Computer Interaction Design, and that you may gain some insight about the processes involved. There will be no financial compensation for your participation in the study.

Consent and Withdrawal: We require your consent before you can participate in the student, which you may indicate by signing your initials in the space provided below. You may choose to withdraw from the study at any time and without explanation, in which case any collected data will be discarded.

Anonymity and Confidentiality: The study involves gaining better general understanding of how students plan their degree programs, but does not involve asking you any specific personal information, nor any specific details of your degree or courses. We do not record or even ask your full name. We will not record or divulge any personal information about you.

By signing with your initials below, you consent to participate in the study.

Initials: LM Date: 03/04/2018

Carleton University, School of Computer Science
COMP3008: Human-Computer Interaction, Winter, 2018

Interaction Design Project User Consent Form

Instructor: Prof. Robert Biddle
Office: HP5169, Tel. Ext. 6317, Email: robert.biddle@carleton.ca

COMP3008 Student Names: ~~Ismail Yussuf~~
Frank Orumn, Ryan Samaroo, Hekla Bagash, Sammy Oramnaglan, Brandon Esford

Note: This project was reviewed by the Carleton University Research Ethics Board (CUREB-B), which provided clearance to carry out the research: (Clearance #105985).

If you have any ethical concerns with the study, please contact Dr. Andy Adler, Chair, Carleton University Research Ethics Board-B (by phone at 613-520-2600 ext. 4085 or via email at ethics@carleton.ca

Study Purpose: This project is to enable students in COMP3008 to experience working with potential users to better understand testing of software using quantitative measures and analysis. Working with potential users is considered best practice in the design of interactive computer systems, and is identified in international standards such as ISO 9241-210:2010 — Human-centred design for interactive systems. Part of the process is first obtaining informed consent from prospective participants, and that is the reason for this form.

Study Procedure: In the project, the proposed system is a kind of password system, where users will be asked to use the system, remember some random passwords, and then try to use them to simulate login to a system. At no time will you be asked for any of your real passwords on any real systems. You will also be asked to fill out a questionnaire about your perceptions of the software and related issues.

Risks, Benefits, Compensation: We are not aware of any risks associated with this study. The benefits are that COMP3008 students gain experience in this aspect of Human Computer Interaction Design, and that you may gain some insight about the processes involved. There will be no financial compensation for your participation in the study.

Consent and Withdrawal: We require your consent before you can participate in the student, which you may indicate by signing your initials in the space provided below. You may choose to withdraw from the study at any time and without explanation, in which case any collected data will be discarded.

Anonymity and Confidentiality: The study involves gaining better general understanding of how students plan their degree programs, but does not involve asking you any specific personal information, nor any specific details of your degree or courses. We do not record or even ask your full name. We will not record or divulge any personal information about you.

By signing with your initials below, you consent to participate in the study.

I.Y Initials: Date: 2018/04/03

Carleton UNIVERSITY
Canada's Capital University

Carleton University, School of Computer Science
COMP3008: Human-Computer Interaction, Winter, 2018

Interaction Design Project User Consent Form

Instructor: Prof. Robert Biddle
Office: HP5169, Tel. Ext. 6317, Email: robert.biddle@carleton.ca

COMP3008 Student Names:

Ryan Samaroo, Heela Bangash, Frerik Drumm, Sammy Diamantstein, Brandon Esford

---

Note: This project was reviewed by the Carleton University Research Ethics Board (CUREB-B), which provided clearance to carry out the research: (Clearance #105985).

If you have any ethical concerns with the study, please contact Dr. Andy Adler, Chair, Carleton University Research Ethics Board-B (by phone at 613-520-2600 ext. 4085 or via email at ethics@carleton.ca

Study Purpose: This project is to enable students in COMP3008 to experience working with potential users to better understand testing of software using quantitative measures and analysis. Working with potential users is considered best practice in the design of interactive computer systems, and is identified in international standards such as ISO 9241-210:2010 — Human-centred design for interactive systems. Part of the process is first obtaining informed consent from prospective participants, and that is the reason for this form.

Study Procedure: In the project, the proposed system is a kind of password system, where users will be asked to use the system, remember some random passwords, and then try to use them to simulate login to a system. At no time will you be asked for any of your real passwords on any real systems. You will also be asked to fill out a questionnaire about your perceptions of the software and related issues.

Risks, Benefits, Compensation: We are not aware of any risks associated with this study. The benefits are that COMP3008 students gain experience in this aspect of Human Computer Interaction Design, and that you may gain some insight about the processes involved. There will be no financial compensation for your participation in the study.

Consent and Withdrawal: We require your consent before you can participate in the student, which you may indicate by signing your initials in the space provided below. You may choose to withdraw from the study at any time and without explanation, in which case any collected data will be discarded.

Anonymity and Confidentiality: The study involves gaining better general understanding of how students plan their degree programs, but does not involve asking you any specific personal information, nor any specific details of your degree or courses. We do not record or even ask your full name. We will not record or divulge any personal information about you.

By signing with your initials below, you consent to participate in the study.

Initials: HB

Date: Apr. 03 2018

Carleton University, School of Computer Science
COMP3008: Human-Computer Interaction, Winter, 2018

Interaction Design Project User Consent Form

Instructor: Prof. Robert Biddle
Office: HP5169, Tel. Ext. 6317, Email: robert.biddle@carleton.ca

COMP3008 Student Names:

Ryan Samaroo, Heela Bangash, Frerik Drumm, Sammy Diamantstein, Brandon Esford

---

Note: This project was reviewed by the Carleton University Research Ethics Board (CUREB-B), which provided clearance to carry out the research: (Clearance #105985).

If you have any ethical concerns with the study, please contact Dr. Andy Adler, Chair, Carleton University Research Ethics Board-B (by phone at 613-520-2600 ext. 4085 or via email at ethics@carleton.ca

Study Purpose: This project is to enable students in COMP3008 to experience working with potential users to better understand testing of software using quantitative measures and analysis. Working with potential users is considered best practice in the design of interactive computer systems, and is identified in international standards such as ISO 9241-210:2010 — Human-centred design for interactive systems. Part of the process is first obtaining informed consent from prospective participants, and that is the reason for this form.

Study Procedure: In the project, the proposed system is a kind of password system, where users will be asked to use the system, remember some random passwords, and then try to use them to simulate login to a system. At no time will you be asked for any of your real passwords on any real systems. You will also be asked to fill out a questionnaire about your perceptions of the software and related issues.

Risks, Benefits, Compensation: We are not aware of any risks associated with this study. The benefits are that COMP3008 students gain experience in this aspect of Human Computer Interaction Design, and that you may gain some insight about the processes involved. There will be no financial compensation for your participation in the study.

Consent and Withdrawal: We require your consent before you can participate in the student, which you may indicate by signing your initials in the space provided below. You may choose to withdraw from the study at any time and without explanation, in which case any collected data will be discarded.

Anonymity and Confidentiality: The study involves gaining better general understanding of how students plan their degree programs, but does not involve asking you any specific personal information, nor any specific details of your degree or courses. We do not record or even ask your full name. We will not record or divulge any personal information about you.

By signing with your initials below, you consent to participate in the study.

Initials:  Date: Apr. 03 2018

Carleton University, School of Computer Science
COMP3008: Human-Computer Interaction, Winter, 2018

Interaction Design Project User Consent Form

Instructor: Prof. Robert Biddle
Office: HP5169, Tel. Ext. 6317, Email: robert.biddle@carleton.ca

COMP3008 Student Names:

Ryan Samaroo, Heela Bangash, Frerik Drumm, Sammy Diamantstein, Brandon Esford

---

Note: This project was reviewed by the Carleton University Research Ethics Board (CUREB-B), which provided clearance to carry out the research: (Clearance #105985).

If you have any ethical concerns with the study, please contact Dr. Andy Adler, Chair, Carleton University Research Ethics Board-B (by phone at 613-520-2600 ext. 4085 or via email at ethics@carleton.ca

Study Purpose: This project is to enable students in COMP3008 to experience working with potential users to better understand testing of software using quantitative measures and analysis. Working with potential users is considered best practice in the design of interactive computer systems, and is identified in international standards such as ISO 9241-210:2010 — Human-centred design for interactive systems. Part of the process is first obtaining informed consent from prospective participants, and that is the reason for this form.

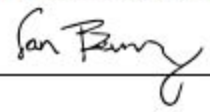
Study Procedure: In the project, the proposed system is a kind of password system, where users will be asked to use the system, remember some random passwords, and then try to use them to simulate login to a system. At no time will you be asked for any of your real passwords on any real systems. You will also be asked to fill out a questionnaire about your perceptions of the software and related issues.

Risks, Benefits, Compensation: We are not aware of any risks associated with this study. The benefits are that COMP3008 students gain experience in this aspect of Human Computer Interaction Design, and that you may gain some insight about the processes involved. There will be no financial compensation for your participation in the study.

Consent and Withdrawal: We require your consent before you can participate in the student, which you may indicate by signing your initials in the space provided below. You may choose to withdraw from the study at any time and without explanation, in which case any collected data will be discarded.

Anonymity and Confidentiality: The study involves gaining better general understanding of how students plan their degree programs, but does not involve asking you any specific personal information, nor any specific details of your degree or courses. We do not record or even ask your full name. We will not record or divulge any personal information about you.

By signing with your initials below, you consent to participate in the study.

Initials:  Date: Apr. 03 2018

Carleton University, School of Computer Science
COMP3008: Human-Computer Interaction, Winter, 2018

Interaction Design Project User Consent Form

Instructor: Prof. Robert Biddle
Office: HP5169, Tel. Ext. 6317, Email: robert.biddle@carleton.ca

COMP3008 Student Names:

Ryan Samaroo, Heela Bangash, Frerik Drumm, Sammy Diamantstein, Brandon Esford

---

Note: This project was reviewed by the Carleton University Research Ethics Board (CUREB-B), which provided clearance to carry out the research: (Clearance #105985).

If you have any ethical concerns with the study, please contact Dr. Andy Adler, Chair, Carleton University Research Ethics Board-B (by phone at 613-520-2600 ext. 4085 or via email at ethics@carleton.ca

Study Purpose: This project is to enable students in COMP3008 to experience working with potential users to better understand testing of software using quantitative measures and analysis. Working with potential users is considered best practice in the design of interactive computer systems, and is identified in international standards such as ISO 9241-210:2010 — Human-centred design for interactive systems. Part of the process is first obtaining informed consent from prospective participants, and that is the reason for this form.

Study Procedure: In the project, the proposed system is a kind of password system, where users will be asked to use the system, remember some random passwords, and then try to use them to simulate login to a system. At no time will you be asked for any of your real passwords on any real systems. You will also be asked to fill out a questionnaire about your perceptions of the software and related issues.

Risks, Benefits, Compensation: We are not aware of any risks associated with this study. The benefits are that COMP3008 students gain experience in this aspect of Human Computer Interaction Design, and that you may gain some insight about the processes involved. There will be no financial compensation for your participation in the study.

Consent and Withdrawal: We require your consent before you can participate in the student, which you may indicate by signing your initials in the space provided below. You may choose to withdraw from the study at any time and without explanation, in which case any collected data will be discarded.

Anonymity and Confidentiality: The study involves gaining better general understanding of how students plan their degree programs, but does not involve asking you any specific personal information, nor any specific details of your degree or courses. We do not record or even ask your full name. We will not record or divulge any personal information about you.

By signing with your initials below, you consent to participate in the study.

Initials:  Date: Apr. 03 2018